Cyber War : Ancaman Baru Keamanan Nasional dan Internasional
(*Cyber War: New National and International Security Threat*)

Adams Pratama Yanuar
Program Studi Ilmu Hubungan Internasional,
UIN Syarif Hidayatullah Jakarta

E-mail : adams.pratama2518@mhs.uinjkt.ac.id

Abstact

Currently, international issues have shifted from traditional issues to non-traditional issues (contemporary). In the past, in the era of World War 1 and 2, physical warfare became a major issue in the international world. However, now that the world has experienced a digital era, the main issue in the international world has shifted from physical warfare to digital warfare or commonly known as Cyber War. Cyber War is a digital war which can be in the form of data robbery or important sector information sectors such as intelligence, national code, foreign policy strategy, national defense, military, etc. So that later the data will be used for the benefit of data thieves. This research will focus on Cyber War Threats on an international scale and the impact that will result from the existence of Cyber War. By using qualitative and quantitative methods, the data presented in this study can be justified. So that this research is considered important enough to add insight and knowledge related to international conditions and threats in the future.

Keywords: Cyber War , Data , Digital Era , Stealing

Abstrak

Isu dunia internasional saat ini telah bergeser dari isu tradisional menjadi isu non tradisional (Kontemporer). Dulu pada era perang dunia 1 dan 2 perang secara fisik masih menjadi isu utama dalam dunia internasional. Namun, saat ini dunia telah mengalami era digital isu utama dalam dunia internasional telah bergeser dari perang secara fisik ke perang digital atau biasa disebut Cyber War. Cyber War merupakan sebuah perang digital yang dapat berupa pencurian data atau informasi sector sector penting seperti Intelejen, Sandi Negara, Strategi kebijakan luar negeri, Pertahanan negara, Militer, dll. sehingga nantinya data tersebut akan dimanfaatkan untuk kepentingan pencuri data. Penelitian ini berfokus pada ancaman Cyber War dalam skala dunia internasional dan dampak

yang akan dihasilkan dari adanya Cyber War. Dengam menggunakan metode kualitatif dan kuantitatif nantinya data yang disajikan di penelitian ini akan dapat dipertanggungjawabkan. Jadi penelitian ini dirasa cukup penting untuk menambah wawasan dan pengetahuan terakit kondisi dunia internasional dan ancaman ancaman di masa yang akan datang.

Kata kunci: Cyber War, Data, Era Digital, Pencurian

Pendahuluan

Dunia saat ini telah mengalami era globalisasi sebagai efek dengan semakin meningkatnya perkembangan teknologi terkhusus internet. Era globalisasi ini telah memunculkan suatu bentuk hubungan yang saling bergantung (*Interdependence*) dan kesalinghubungan (*Interconnection*) antar negara-bangsa dan aktor-aktor internasional yang terintegrasi secara global.

Interdepedensi dan interkoneksi mempunyai dua konsekuensi penting yaitu, isu isu politik internasional telah melebar tidak lagi semata-mata menyangkut ancaman perang nuklir, persaingan ideologi komunisme dengan kapitalisme, krisis diplomasi dan lain sebagainya. Kedua, globalisasi yang dicirikan oleh integrasi melahirkan suatu fenomena dan persoalan baru yang tidak dapat diselesaikan oleh masing-masing negara nasional sendirian, tetapi harus diselesaikan secara bersama-sama sebagai komunitas warga dunia.[1]

Dari konsekuensi pertama menyebabkan melebarnya isu-isu dalam politik internasional dengan seiring meningkatnya penggunaan teknologi internet di seluruh belahan dunia meningkat pula kejahatan atau penyalahgunaan yang dilakukan melalui internet yang biasa disebut perang siber (c*yber war*). *Cyber war* atau *cyber crime* merupakan perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi.

Sebuah lembaga pencegahan kejahatan, di Havana, Cuba pada tahun 1999 dan di Wina, Austria pada tahun 2000, menyebutkan terdapat dua (2) pengertian *cyber crime* secara garis sempit luas. *Cyber crime* dalam arti sempit, yaitu prilaku ilegal / melanggar yang secara langsung menyerang sistem keamanan komputer dan data yang diproses oleh computer. Adapun *Cyber crime* dalam arti luas, yaitu prilaku ilegal/ melanggar yang berkaitan dengan sistem komputer atau jaringan.[2]

Cyber crime mempunyai beberapa bentuk yaitu hacking, *cracking, carding*, *Cyber Sabotage*, *cyber attack, spywar*, dan lain-lain. Semua bentuk kejahatan ini dapat

[1] Budi Winarno. *Dinamika Isu-isu Global Kontemporer.* (Yogyakarta: CAPS. 2014). hal xix

[2] Deky Rosdiana. 2013. "Cyber Warfare Menjadi Ancaman NKRI di Masa Kini dan Masa Depan". Kompasiana, 23 September 2013. https://www.kompasiana.com/deky91/5528eab76ea8346b-368b45c9/cyber-warfare-menjadi-ancaman-nkri-di-masa-kini-dan-masa-depan)

sewaktu-waktu mengancam keamanan internasional sehingga setiap negara mestilah menyiapkan konsep *cyber security* sebagai tameng dan pertahanan dalam menangggulangi ancaman *cyber crime*.

Namun, dikarenakan ancaman *cyber crime* ini merupakan ancaman internasional yakni tidak hanya satu negara saja yang mengalami, sehingga dirasa perlu untuk setiap negara di dunia berkolaborasi dalam menanggulangi *cyber crime*. Selain itu negara harus melibatkan institusi internasional dalam mencari *Cyber security* guna bersiap siap menghadapi ancaman *cyber crime* pada saat-saat tertentu.

Tulisan ini bertujuan untuk menganalisis ancaman dunia internasional di saat ini dan masa depan salah satunya ancaman *Cyber war / Cyber crime*. Selain itu juga menguji seberapa jauh ancaman tersebut mengancam keamanan dunia internasional yang sejauh ini sedang dibangun sedikit demi sedikit dan menguji seberapa bahaya c*yber crime* ini terhadap masyarakat internasional. Semoga tulisan ini berguna bagi semua yang ingin melakukan penelitian terkait *cyber crime* dan ancaman keamanan dunia internasional kontemporer. Penulis menyadari sangat banyak kekurangan terhadap tulisan ini, namun penulis akan terus berusaha untuk menampung saran dan kritik sembari memperbaiki tulisan ini.

Kajian Pustaka dan Kerangka Pemikiran

Cyberspaces

Dalam buku komunikasi militer yang diterbitkan oleh asosiasi pendidikan tinggi ilmu komunikasi pada bagian "*perang cyber dalam dinamika komunikasi internasional*" yang ditulis oleh M Badri, dijelakan secara terperinci tentang konsep *cyber spaces*. Dengan berkembangnya teknologi dan komunikasi dalam tatanan dunia internasional, nyatanya ranah teknologi pun dijadikan media baru untuk peperangan (*Cyber War*).

Dengan teknologi yang maju saat ini aktivitas yang terjadi di dimensi nyata (*real space*) bertransformasi ke dimensi dunia maya (c*yber spaces*) termasuk peperangan. Era peperangan saat ini bukan lagi tentang peperangan secara fisik, namun peperangan melalui dunia maya (*cyber spaces*). Hal ini dapat menjadi ancaman bagi keamanan internasional dan ketertiban dunia.

Saat ini *cyber spaces* telah menjadi wadah potensial untuk memulai pertempuran yang mengancam keamanan internasional. Pihak yang berseteru tentunya bukan hanya negara, tetapi di elemen akar rumput seperti masyarakat juga mengalami perseteruan. Mereka saling berhadapan melalui ajang perdebatan satu sama lain, penyebaran upaya dominasi informasi hingga kegiatan yang bersifat destruktif seperti *web destroying rally* sebagai cara *purposeful publicity* dan intimidasi atau yang lebih berat lagi. Perseteruan ini tidak hanya melibatkan pelaku amatir, tapi juga mereka yang punya keterampilan dan kemampuan khusus bahkan tidak sedikit juga

kelompok kelompok profesional yang menawarkan jasa layaknya pasukan bayaran.[3]

Dengan adanya *cyber spaces* ini semakin menandakan bahwa konsep keamanan internasional telah bertransformasi dari keamanan tradisonal menjadi keamanan non-tradisional. Era keamanan tradsional yang banyak membahas isu-isu *high politics* dan aktornya disentralkan kepada negara telah bertansformasi menjadi keamanan non-tradisional yang berfokus pada *human security*.[4]

Human security mencakup berbagai dimensi keamanan, seperti keamanan ekonomi, keamanan pangan, keamanan kesehatan, keamanan lingkungan, keamanan personal, keamanan politik.[5] Dari definisi di atas, *cyber spaces* dapat kita kategorikan sebagai kejahatan yang dapat mengancaman keamanan non-tradisional dikarenakan dapat mengancam *human security* masyarakat internasional, terutama keamanan personal informasi pribadi dari setiap individu masyarakat internasional. Kita tahu saat ini bahwa informasi personal kita sangat rentan disalahgunakan oleh perusahaan-perusahaan seperti *facebook*, *whatsapp*, dan lainnya.

Lebih dari itu data rahasia negara juga dapat diambil sewaktu-waktu oleh negara lain dan dapat disalahgunakan dengan melakukan *cyber threat*. Sebagai contoh serangan *cyber* yang dilancarkan Rusia terhadap Estonia , sebagai respon atas kebijakan pemerintah Estonia yang memutuskan untuk memindahkan patung perunggu yang sangat berharga bagi Rusia karena menandakan bahwa Estonia pernah menjadi bagian dari Uni Soviet, namun berbeda dengan Estonia yang menganggap patung tersebut sebagai bentuk penjajahan dan penindasan. Itulah sebabnya pemerintah Estonia kemudian membuat kebijakan untuk memindahkan patung tersebut.

Namun berita yang beredar di media berbahasa Rusia mengatakan, monumen tersebut diluluhlantahkan, bersamaan dengan kuburan pasukan bersenjata Soviet yang gugur dalam perang. Informasi itu membuat warga Rusia Estonia marah, sehingga berujung pada terjadinya kerusuhan dimana-mana. Tidak hanya itu selain kerusuhan Estonia juga mengalami ancaman lain Botnets media massa, perusahaan telekomunikasi, kementerian-kementrian, membanjiri bank dan lembaga eksekutif Estonia dengan spam dan menyebarkan serangan *DDoS* atau *Denial-of-Service*.

Estonia telah membangun kembali teknologinya sejak kemerdekaannya. Sebagai negara *cyber* yang dapat dikatakan sangat paham teknologi, mengalami ancaman akibat kelemahannya, karena beberapa serangan berlanjut selama beberapa minggu. Lebih dari 50 situs web utama *offline* sekaligus. Mesin kasir otomatis dan *email* resmi pemerintah berhenti bekerja. Selain itu, orang Estonia juga tidak dapat mengakses media untuk mencari tahu apa yang sedang terjadi, karena wartawan tidak dapat menggunakan web dan internet untuk melaporkan atau menyampaikan berita.

---

3 Rosa Ariani Sukamto dan M. Shalahuddin. *Modul Pembelajaran Rekayasa Perangkat Lunak (Terstruktur dan Beror ientasi Objek).* (Bandung: Modula. 2011) h.4

4 Budi Winarno. *op. cit*, 8-9

5 UNDP. 1994. "Human Development Report". (UNDP:1994)

Setelah ditelusuri lebih lanjut, ternyata serangan tersebut berasal dari Rusia.[6]

Hal ini menjadi salah satu contoh betapa mengerikannya *cyber war* dan besarnya kerugian yang di rasakannya sehingga dirasa perlu sebuah negara mempunyai *cyber security* guna menjadi tameng jika sewaktu-waktu datang serangan *cyber*, sehingga konsep keamanan dianggap penting dimiliki setiap negara untuk keamanan nasionalnya.

Teori Sekuritisasi

Sebelumnya telah saya singgung sedikit terkait dengan *cyber security* yang harus dimiliki oleh setiap negara guna mempertahankan keamanan nasionalnya. Pada bagian ini akan dibahas lebih lanjut terkait dengan teori sekuritisasi yang dipelopori oleh Barry Buzan sebagaimana ditulis dalam bukunya yang berjudul *Security: A Framework for Analysis*. Teori yang dipelopori Buzan ini diartikan bahwa suatu isu menjadi masalah keamanan, karena ada aktor-aktor yang merencanakannya dengan mengatakan bahwa isu tersebut merupakan ancaman bagi suatu objek. Teori sekuritisasi ini mempunyai tiga model dalam mengkaji *sector cyber* secara spesifik, yaitu:

a. *Hypersecuritization*: Model yang dipergunakan untuk mendeskripsikan ancaman dan bahaya dari serangan lewat jaringan sebuah negara di atas level normal. Jaringan yang rusak, menyebabkan kerugian besar terhadap banyak sektor terutama finansial dan militer.
b. *Everyday Security Practice*: dimaksudkan untuk mengamankan aktor, termasuk organisasi privat dan bisnis, memobilisasi individu "normal" mengamankan kemitraan individu dan pemenuhan dalam menjaga jaringan keamanan serta membuat skenario *hypersecuritization* lebih rasional dengan strategi menggabungkan perangkat perangkat skenario ancaman dan pengalaman yang sudah tidak asing lagi dalam kehidupan sehari-hari.
c. *Technification*: menggunakan pakar-pakar dalam bidang teknologi *cyber* yang akan memainkan peran besar dalam *hypersecuritization*.

Metode penelitian

Penelitian ini berfokus pada macam-macam kejahatan *cyber* yang pernah terjadi di dunia hingga hari ini. Dari objek penelitian ini nantinya akan dianalisis seberapa bahayanya kejahatan *cyber* ini dan seberapa besar kemungkinannya dalam mengganggu keamanan internasional.

Penelitian ini menggunakan metode kualitatif dengan menggunakan sumber sumber sekunder dari beberapa sumber bacaan seperti buku, jurnal, portal berita, dll yang tentunya berfokus pada kajian-kajian tentang *cyber war* dan keamanan internasional. Penulis sadar bahwa penelitian ini masih banyak sekali kekurangannya dan penulis sangat berharap atas kritik dan saran dari para pembaca

[6] https://www.qureta.com/post/serangan-siber-yang-berawal-dari-patung-1

untuk mengevaluasi diri penulis dalam melakukan penelitian ke depannya. Penulis berharap nantinya penelitian ini dapat bermanfaat bagi para pembaca, terutama dalam mengkaji tentang *cyber war* dan kejahatan kejahatan *cyber* yang dapat menggangu keamanan internasional dan ketertiban dunia yang telah dibangun sedemikian rapih dan kokoh.

Pembahasan

Di era digital saat ini teknologi menjadi hal yang sangat vital di tengah masyarakat Internasional. Teknologi, terkhusus internet, menjadi salah satu kebutuhan manusia abad ini disamping kebutuhan sandang, pangan, dan papannya. Dengan demikian setiap negara harus mampu menguasai, mengkontrol, dan mengendalikan pergerakan internet warga negaranya. Bagaimana tidak, menurut data yang disampaikan oleh *Weare Social* dan *Hootsuite* tentang lanskap digital dunia terungkap bahwa penggunaan internet di seluruh dunia mencapai angka 4,5 milyar orang. Angka ini menunjukkan bahwa pengguna internet telah mencapai lebih dari 60 persen penduduk dunia atau lebih dari separuh populasi bumi.[7] Dari jumlah tersebut sebanyak 3,8 milyar telah menggunakan *social media.* Berdasarkan data ini kita dapat menggambarkan bahwa saat ini social media telah menjadi dunia baru bagi masayarakat dunia disamping dunia yang sebenarnya.

Terlebih di *era pandemic* ini dimana beberapa sektor bertransformasi dengan menggunakan media online dalam proses pengerjaannya. Mulai dari sector pendidikan, sektor bisnis, perdagangan dll. Sebagai contoh di Indonesia, menurut penyedia jasa internet *indihome* selama pandemik covid-19 ini permintaan untuk pemasangan wifi meningkat sebanyak 30 sampai 40 persen. Menurut Asosiasi penyelenggara jasa internet Indonesia, kenaikan trafik penggunaan internet dari sebelumnya sekitar 20 – 25%.[8]

Dapat disimpulkan bahwa internet saat ini telah menjadi kebutuhan pokok dari setiap individu di dunia ini, terlebih di masa *pandemik*. Karna mau tidak mau sektor-sektor vital bertansformasi menjadi online seperti sekolah, pekerjaan dan aktivitas jual beli, sehingga semua masyarakat dunia saat ini harus mulai beradaptasi dengan kehidupan di era internet saat ini.

Namun meningkatnya penggunaan internet mempunyai dampak negatif terhadap keamanan individu dan keamanan dunia internasional saat ini. Salah satu dampak negatifnya adalah semakin masifnya penyebaran *hoax*, provokasi dan pencurian informasi.[9] Badan Siber dan Sandi Negara (BSSN) bahkan telah mencatat

---

7 Bagus Ramadhan. 2020. "*Ini Data Pengguna Internet di Seluruh Dunia Tahun 2020.*" Teknoia.com, 13 Februari 2020. https://teknoia.com/data-pengguna internet-dunia-ac03abc7476

8 Agus Tri Haryanto.2020. "*APJII Sebut Jumlah Pengguna Internet di Indonesia Naik Saat Pandemi*". Detik.com (inet.detik), 30 September 2020. https://inet.detik.com/telecommunication/d-5194182/apjii-sebut-jumlah-pengguna-internet-di-indonesia-naik-saat-pandemi

9 Amarmuazam usmani bin Othman. 2017. "*Analisis Penggunaan Media Siber Terhadap Keamanan Nasional : Suatu Studi di Malaysia*" Dalam jurnal *Jurnal Prodi Strategi Pertahanan Darat* Universitas Pertah-

selama pandemik ini (Periode Januari – April 2020) telah terjadi 88.414.296 serangan siber. Serangan tersebut terjadi dalam rentang waktu 1 Januari hingga 12 April 2020. Pada bulan Januari terpantau 25.224.811 serangan yang terjadi dan kemudian pada bulan Februari tercatat 29.188.645 serangan. Pada bulan Maret terjadi 26.423.989 serangan. Sampai dengan 12 April 2020 tercatat 7.576.851 serangan. Puncak jumlah serangan terjadi pada tanggal 12 Maret 2020 yang mencapai 3.344.470 serangan. Namun, setelah itu jumlah serangan mengalami penurunan yang cukup signifikan saat diberlakukannya kebijakan *work from home* (WFH) di berbagai sector mulai dari pendidikan, bisnis, dll.

Namun demikian selama WFH berlangsung telah terjadi beberapa serangan siber yang memanfaatkan isu terkait dengan Covid-19. Jenis serangan yang paling banyak adalah *trojan activity* sebanyak 56% dan kemudian disusul dengan aktifitas *information gathering* (pengumpulan informasi) sebesar 43% dari total keseluruhan serangan, sedangkan 1% sisanya merupakan *serangan aplikasi web.*[10] Hal ini membuktikan dari adanya peningkatan penggunaan internet berdampak pula pada peningkatan terjadinya serangan siber.

Lebih dari itu, hal tersebut akan lebih memperbesar potensi terjadinya perang siber antara negara maupun serangan siber dengan aktor bukan negara. Terdapat beberapa contoh efek dari penggunaan internet terhadap stabilitas keamanan internasional, antara lain:

a. Serangan ke Estonia

Pada 27 April 2007, serangan siber yang cukup besar melanda Estonia. Sasaran serangan tersebut adalah institusi penting setempat seperti legislatif, perbankan, kementerian, hingga media massa. Kebanyakan serangan berjenis penyebaran *denial of service* dengan berbagai macam strategi.

Selain itu, metode *spamming* dan *deface* juga banyak dilakukan oleh para pelakunya. Beberapa pengamat menganalisis bahwa serangan ini adalah salah satu yang paling kompleks dan sistematis. Banyak yang beranggapan pelakunya didukung oleh negara. Dalam hal ini, tuduhan mengarah ke Rusia. Diduga serangan tersebut dilakukan sebagai protes kebijakan Perdana Menteri Andrus Ansip. Protes terjadi karena Ansip membongkar sebuah monumen tentara Rusia dari ibu kota Estonia.

Menteri luar negeri Estonia, Urmas Paet menyimpulkan bahwa Rusia terlibat secara langsung dalam serangan siber tersebut. Namun, beliau tidak mampu mengajukan bukti kuat dan pihak Rusia pun membantah tuduhan tersebut.

---

anan Volume 3 No 3.
http://jurnalprodi.idu.ac.id/index.php/SPD/article/view/134

10 BSSN. 2020. "*Rekap Serangan Siber Januari – April 2020*". bssn.go.id, 20 April 2020. https://bssn.go.id/rekap-serangan-siber-januari-april-2020/; diakses Oktober 2020

b. Serangan terhadap nuklir Iran

Pada tahun 2010 sebuah virus jaringan yang sangat canggih, yakni Stuxnet, menyerang fasilitas nuklir Iran. Awalnya, Stuxnet diyakini hanya sebagai *worm* biasa yang lumayan canggih. Tapi, peneliti kemudian menemukan worm itu menargetkan sistem khusus '*supervisory control and data acquisition'* (SCADA).

SCADA digunakan untuk memanajemen sistem pipa, perangkat manufaktur dan pembangkit listrik tenaga nuklir (PLTN). Karena kecanggihan yang dimiliki virus tersebut, Stuxnet kemungkinan besar adalah buatan dari Negara.

Lebih jauh lagi, peneliti menemukan bahwa Stuxnet dirakit untuk melakukan pencegahan perintah spesifik dari SCADA ke fungsi spesifik. Meski belum bisa dipastikan sasaran pastinya apa, namun temuan terbaru menguatkan dugaan bahwa target utamanya adalah PLTN Natanz atau Bushehr di Iran. Presiden Iran, Mahmoud Ahmadinejad, menyampaikan bahwa serangan virus Stuxnet berdampak pada fasilitas nuklir Iran. Beberapa kerusakan diakui telah terjadi.[11]

c. Pencurian data besar besaran terhadap Singapura

Serangan siber terbesar telah terjadi pada tahun 2018 menyerang negara kota tersebut. Data pribadi sekitar 1,5 juta warga Singapura termasuk data pribadi Perdana Menteri Lee Hsien Loong telah dicuri dalam serangan siber yang terjadi sejak akhir Juni 2018.

Pemerintah Singapura tak menyebutkan identitas lengkap pecuri data tersebut. Hanya saja dari serangannya memiliki ciri khas bahwa kelompok pencuri data tersebut berasal dari suatu negara. Menurut pihak berwenang Singapura seperti dikutip *Reuters,* pada akhir Juni 2018, adapun data yang dicuri oleh peretas ialah berupa data pribadi dan juga catatan resep dari klinik rawat jalan di Singapura.

Tak tangung-tanggung, data yang diambil tersebut merupakan data sejak 3 tahun sebelum 2018. Pada Senin (6/8/2018), Menteri Komunikasi dan Informasi Singapura mengatakan, pemerintah tidak akan mengungkapkan identitas peretas demi alasan keamanan personal. Tetapi serangan tersebut adalah aktivitas dari kelompok "Advanced Persistent Threat" (APT) yang biasanya berafiliasi dengan negara.[12]

Dari beberapa contoh di atas semakin memperkuat argumen saya di awal bahwa potensi meledaknya *cyber war* semakin besar terlebih di masa pandemik seperti ini dengan penggunaan internet yang semakin meningkat tanpa dibarengi den-

---

[11] Detik.com. 2012. "*Serangan Cyber yang Menghebohkan Dunia". Detik.com 7 November 2012.* https://inet.detik.com/security/d-2084499/7-serangan-cyber-yang-menghebohkan-dunia/8; Diakses Oktober 2020

[12] Khomarul Hidayat. 2018. "Serangan Siber Terbesar dalam Sejarah Menyerang Singapura". Kontan.co.id. 6 Agustus 2018. https://investasi.kontan.co.id/news/serangan-siber-terbesar-dalam-sejarah-menyerang-singapura

gan edukasi penggunaannya. Oleh karena itu, dirasa perlu untuk mencari elemen proteksi diri oleh setiap negara dengan berbasis c*yber* sehingga setiap negara nantinya akan memilki *cyber security* masing-masing yang membuat negara akan aman dari ancaman serangan *cyber* .

Selain itu negara juga harus mencari elemen proteksi dunia internasional dari ancaman *cyber war*, harus ada *cyber security* internasional sehingga nantinya *cyber security* ini akan menjaga stabilitas keamanan internasional dan menghindarkan dunia internasional dari terjadinya *cyber war*. Adapaun beberapa alternative dari *cyber secutiry* akan dibahas dibagian selanjutnya, alternative-alternative ini telah dipraktekan di beberapa negara dan semoga bisa menjadi referensi baik secara individu maupun negara .

Cyber Security

Cyber security merupakan upaya untuk memastikan pencapaian dan pemeliharaan kondisi keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan Siber. Tujuan keamanan umum terdiri dari: ketersediaan; integritas dan terjaminnya data personal warga negara dari adanya serangan siber dari oknum oknum.

Dalam lingkup internasional terdapat konsep bersama dalam menanggulangi adanya serangan siber, yaitu Global cyber-security. Global *cyber-security* dibangun di atas lima bidang kerja: Pertama, elemen kepastian hukum (undang-undang *cyber crime*). Kedua, elemen teknis dan tindakan prosedural (sebuah aksi konkrit dalam menanggulangi serangan siber). Ketiga, elemen struktur organisasi (struktur organisasi yang berperan dalam *cyber security*). Keempat, elemen *capacity building* dan pendidikan Pengguna (kampanye publik dan edukasi terhadap *cyber security*). Kelima, elemen kerjasama internasional (termasuk didalamnya kerja sama timbal balik dalam upaya mengatasi ancaman *cyber*).

Elemen-elemen tersebut merupakan elemen yang telah dilakukan Indonesia hingga saat ini. Dari sini nantinya kita dapat mengevaluasi atas apa yang telah dikerjakan Indonesia sejauh ini terhadap *Cyber Security* dan nantinya penulis akan mengkomparasikan *cyber security* yang dilakukan Indonesia dengan negara lain yakni Amerika sebagai negara yang sangat berganting pada internet dan mempunyai andil besar terhadap perkembangan internet hingga saat ini. Adapun strategi Indonesia dalam menghadapi ancaman cyber security, antara lain:

1. Kepastian Hukum

Indonesia mempunyai beberapa aturan hukum, yakni Peraturan Menteri Komunikasi dan Informatika No.26/PER/M.Kominfo/5/2007 yang berkaitan dengan Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet yang kemudian direvisi dengan Peraturan Menteri Komunikasi dan Informatika No.16/PER/M.KOMINFO/10/2010 yang kemudian diupdate kembali dengan Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.KOMIN-

FO/12/2010.

Salah satu *ouput* dari peraturan tersebut adalah pembentukan ID-SIRTII (*Indonesia Security Incident Response Team on Internet Infrastructure*) yang merupakan sebuah tim yang ditugaskan Menteri Komunikasi dan Informatika (Kominfo) untuk membackup pengawasan keamanan protokol berbasis internet.

2. Teknis dan tindakan procedural

   Terkait dengan elemen kedua ini, teknis dan tindakan prosedural, butuh adanya aksi nyata dari setiap aktor aktor cyber security yang terkait dengan keamanan informasi, standar infrastruktur yang wajib dipenuhi yang sesuai dengan standar internasional dalam menghadapi *cyber war* termasuk didalamnya adanya perimeter defense yang memadai, adanya system monitor jaringan, system information and event management yang berfungsi memonitor berbagai kejadian di jaringan terkait dengan insiden keamanan, network security assement yang berperan sebagai control dan pemelihara keamanan.

3. Struktur Organisasi

   Demi mewujudkan *cyber security*, Kementrian Pertahanan telah menyusun elemen struktur organisasi dengan membentuk Tim Kerja Pusat Operasi Dunia Maya (*Cyber Defence Operation Centre*) yang bertujuan untuk menjaga keamanan dan perlindungan keamanan internal (Kemhan) dan juga keamanan eksternal yaitu negara Indonesia itu sendiri. Pembentukan *Cyber Defence Operation Centre* dalam tugas *cyber security*-nya secara spesifik ditugaskan untuk membangun system pertahanan yang berbasis melibatkan seluruh elemen nasional seperti warga negara, wilayah, dan sumber daya nasional untuk menegakkan kedaulatan negara, keutuhan wilayah dan keselamatan segenap bangsa dari ancaman cyber.[13]

4. Capacity building

   Dalam aspek peningkatan kapasitas SDM, TNI mengambil peran yang cukup sentral disini. TNI sebagai pilar pertama dalam perwujudan keamanan –dalam hal ini keamanan *cyber*– telah melakukan kerjasama dengan stakeholder yang memililki kemampuan dibidang teknologi informasi yaitu Institut Teknologi Del (IT Del), Sumatera Utara. Kerjasama ini diwujudkan dalam bentuk tiga program antara lain, penyiapan model perang cyber, seminar *military cyber intelligence and cyber operation*, serta *cyber camp* atau *pekan cyber*.[14]

5. Kerja sama Internasional

   Di elemen ini Indonesia telah menjalankan beberapa kerjasama dalam rangka penanggulangan *cyber crime* yang telah dilakukan diantaranya dengan menjadi anggota menjadi anggota International Telecommunication Union (ITU), menjadi *steering committee* Asia Pacific Computer Emergency Response Team (APCERT),

---

[13] Erfan Syah. 2012. "*Kemhan dan TNI Bangun Pertahanan Cyber.*" Artileri.org, 29 November 2012. https://www.artileri.org/2012/11/kemhan-dan-tni-bangun-pertahanan-cyber.html diakses oktober 2020

[14] Indra Wijaya. 2014. "TNI AD Gandeng IT Del Bangun Cyber Defense". Tempo.co, 13 Mei 2014. https://nasional.tempo.co/read/577268/tni-ad-gandeng-it-del-bangun-cyber-defence/full&view=ok

ASEAN Network Security Action Council (ANSAC), anggota dari Forum of Incident Response and Security (FIRST), dan dalam beberapa kesempatan melakukan kerjasama bilateral dengan negara negara yang cyber securitynya dapat dikatakan sudah lebih *advance* dibanding Indonesia.

Terkait dengan kerjasama internasional dalam bidang *cyber-security*, Indonesia juga ikut berperan aktif dalam program *Global Cyber Security Agenda* (GSA) yang diluncurkan pada *World Telecommunication and Information Society Day 2007* yang merupakan program kerjasama internasional yang bertujuan untuk menciptakan strategi dan solusi untuk meningkatkan kepercayaan dan keamanan di tengah masyarakat informasi.[15]

Lima hal tersebut telah dijalankan Indonesia sejauh ini. Namun , berdasarkan laporan Badan Siber dan Sandi Negara (BSSN) merekam masih adanya 88.414.296 serangan siber yang telah terjadi di Indonesia sejak 1 Januari sampai dengan 12 April 2020.[16] Data tersebut menunjukkan bahwa Indonesia masih termasuk negara yang rentan atas ancaman *cyber crime*.

Sementara itu, strategi dari Amerika serikat dalam menanggulangi ancaman *cyber crime* di negaranya, sebagai perbandingan yang dapat dijadikan alternatif strategi Indonesia guna memperkuat pertahanan *cyber* nasionalnya, antara lain:

1. Executive Order 13587 - *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*

   Pada tahun 2011, Presiden AS mengeluarkan perintah eksekutif langsung tentang reformasi struktural untuk meningkatkan keamanan jaringan *cyber* dan berbagi tugas dan tanggung jawab dalam mengamankan informasi rahasia. Terdapat beberapa bagian dalam *executive order* ini, diantaranya:
   a) Memerintahkan reformasi struktural dalam mengamankan informasi rahasia;
   b) Tanggung jawab umum agen;
   c) Membuat komite senior pengamanan dan pembagian informasi rahasia;
   d) Membangun kantor pengamanan dan pembagian informasi rahasia;
   e) Memilih agen eksekutif pengamanan dan pembagian informasi rahasia pada jaringan komputer, dalam bagian ini dapat disebut mata-mata;
   f) Mengadakan satuan tugas untuk mengahadapi ancaman;
2. Presidential Proclamation - *National Cyber security Awareness Month, 2014*

   Sebagai inisiator peringatan bulan kesadaran *Cyber security nasional*, Presiden Barack Obama menyadari bahwa Amerika merupakan negara yang sangat bergantung pada teknologi, komunikasi, dan informasi terlebih internet. Di sinilah perlunya perhatiaan oleh setiap masyarakat atas urgensi adanya *Cyber security*.

---

[15] Menteri Kominfo Pada "High Level Segment ITU Council2008" Yang Membahas Cyber security,(http://www.postel.go.id/info_view_c_26_p_814.html Diakses oktober 2020)

[16] Retia Kartika Dewi. 2020. " BSSN Catat Adanya 88,4 Juta Serangan Siber Selama Pandemi Corona". Kompas.com, 23 April 2020. https://www.kompas.com/tren/read/2020/04/23/165400665/bssn-catat-adanya-88-4-juta-serangan-siber-selama-pandemi-corona?page=all

Tujuan dari diadakannya bulan peringata *cyber security* nasional adalah guna mendongkrak perhatian dari setiap lapisan masyarakat untuk berperan aktif dalam menjaga Amerika dari serangan siber eksternal. Tidak hanya peringatan, pada bulan tersebut juga dilaksanakan program sosialisasi, edukasi, kampanye publik, agar setiap masyarakat semakin peka urgensi dari *Cyber security* nasional.

Penutup

Cyber war merupakan ancaman masa depan dalam keamanan internasional dan nasional seiring dengan meningkatnya penggunaan internet dan era globalisasi. Indonesia telah menjalankan beberapa strategi dalam menanggulangi dampak *cyber war,* mulai dari membuat undang-undang keamanan siber hingga menempuh jalan kerja sama internasional. Namun demikian, hal tersebut masih kurang efektif, karena hingga April 2020 tercatat adanya 88 juta kejahatan *cyber* di Indonesia. Dalam kaitan itu, strategi yang telah dilakukan Amerika Serikat pada masa pemerintahan Barrack Obama dapat menjadi alternatif perbandingan dan diadopsi sebagai strategi dalam penanggulangan ancaman kejahatan *cyber war* di masa depan.

Daftar Pustaka

Ardiyanti, Handriyani. 2016 "Cyber-Security dan Tantangan Pengembangannya Di Indonesia" dalam jurnal politica Vol 5 no 1 https://jurnal.dpr.go.id/index.php/politica/issue/view/104

Attahriq, Hakka. Serangan Siber yang Berawal dari Patung (https://www.qureta.com/post/serangan-siber-yang-berawal-dari-patung-1) Diakses agustus 2020

Badri , Muhammad , 2011 , *Perang cyber dalam dinamika komunikasi internasional dalam buku Komunikasi militer* , Aspikom

BSSN. 2020. "Rekap Serangan Siber Januari – April 2020". bssn.go.id. 20 April 2020. (https://bssn.go.id/rekap-serangan-siber-januari-april-2020/) Diakses Oktober 2020

Buzan, Barry. 1998. *Security: A Framework for Analysis*. Boulder: Lynne Reinner Publishers.

Chansoria, Monika (2012) "Defying Borders in Future Conflict in East Asia: Chinese Capabilities in The Realm of Information Warfare and Cyber Space", The Journal of East Asian Affairs, Vol.26 No. 1. Seoul: Institute for National Security Strategy, hlm. 106-107

Dewi, Retia Kartika. "*BSSN Catat Adanya 88,4 Juta Serangan Siber Selama Pandemi Corona*". Kompas.com, 23 April 2020. https://www.kompas.com/tren/read/2020/04/23/165400665/bssn-catat-adanya-88-4-juta-serangan-siber-selama-pandemi-corona?page=all

Gautama, Hasyim. 2020. "*Penerapan Cyber Security*, http://kemhubri.dephub.go.id/pusdatin/files/materi/Penerapan_Cyber security.pdf, diakses Oktober 2020

Haryanto., Agus Tri. 2020. "APJII Sebut Jumlah Pengguna Internet di Indonesia Naik Saat Pandemi". Detik.com (inet.deti), 30 September 2020. https://inet.detik.com/

telecommunication/d-5194182/apjii-sebut-jumlah-pengguna internet-di-indonesia-naik-saat-pandemi) Diakses Agustus 2020

Hidayat, Khomarul. Serangan siber terbesar dalam sejarah menyerangSingapura(https://investasi.kontan.co.id/news/serangan-siber-terbesar-dalam-sejarah-menyerang-singapura) Diakses Oktober 2020

Indra Wijaya. 2014. "TNI AD Gandeng IT Del Bangun Cyber Defense". Tempo.co, 13 Mei 2014. https://nasional.tempo.co/read/577268/tni-ad-gandeng-it-del-bangun-cyber-defence/full&view=ok

Menteri Kominfo Pada "High Level Segment ITU Council2008" Yang Membahas Cyber security,(http://www.postel.go.id/info_view_c_26_p_814.html Diakses oktober 2020)

Othman, Amarmuazam Usmani bin. 2017. "Analisis Penggunaan Media Siber Terhadap Keamanan Nasional : Suatu Studi di Malaysia" Dalam jurnal Jurnal Prodi Strategi Pertahanan Darat Universitas Pertahanan Volume 3 no 3file:///C:/Users/User/AppData/Local/Temp/134-906-1-PB-1.pdf

Ramadhan., Bagus. Ini Data Pengguna Internet di Seluruh Dunia Tahun 2020Berdasarkan laporan Digital 2020 yang dilansir We Are Social dan Hootsuite. (https://teknoia.com/data-penggunainternet-dunia ac03abc7476) Diakses Agusutus 2020

Rosdiana, Deky. 2013. "*Cyber Warfare Menjadi Ancaman NKRI di Masa Kini dan Masa Depan"*. Kompasiana, 23 September 2013. https://www.kompasiana.com/deky91/5528eab76ea8346b368b45c9/cyber-warfare-menjadi-ancaman-nkri-di-masa-kini-dan-masa-depan. Diakses Agustus 2020

Saputra., Moehammad Yuliansyah dan Tri Joko Waluyo 2015 "Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancaman Cyber." Jurnal Online Mahasiswa Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Riau, Vol 2/2. https://jom.unri.ac.id/index.php/JOMFSIP/article/view/7446

Serangan *Cyber* yang Menghebohkan Dunia (https://inet.detik.com/security/d-2084499/7-serangan-cyber-yang-menghebohkan-dunia/8) Diakses Oktober 2020

Sukamto., Rosa Ariani & M. Shalahuddin. *Modul Pembelajaran Rekayasa Perangkat Lunak (Terstruktur dan Berorientasi Objek)*. (Bandung: Modula. 2011)

Syah., Erfan. 2012. "*Kemhan dan TNI Bangun Pertahanan Cyber*." Artileri.org, 29 November 2012. https://www.artileri.org/2012/11/kemhan-dan-tni-bangun-pertahanan-cyber.html diakses oktober 2020

UNDP. 1994. "Human Development Report." (UNDP:1994) Diakses Oktober 2020

Winarno., Budi. *Dinamika Isu-isu Global Kontemporer. (*Yogyakarta: CAPS. 2014)