KEJAHATAN SIBER TRANSNASIONAL DAN STRATEGI PERTAHANAN SIBER INDONESIA

Ahmad Saudi
FISIP Universitas Riau, Kampus Bina Widya Km. 12,5 Simpang Baru Panam, Pekanbaru 28293

Abstract: This study aims to explain how the influence of transnational cyber crimes against Indonesian cyber defense strategy. In this study also tried to explain the Indonesian government's strategy in responding to the crime of cross country cadres. The level of analysis of this research is the country as an international actor. This study uses a realist perspective and uses the theory of security to explain the problem in this cyber crime. This research is qualitative research. Technique of collecting data of this research is literature study. The result of this research is the Indonesian government has strategies to overcome the influence of transnational cyber crime. The Indonesian strategy is the policy of national cyber defense security.

Abstrak: Penelitian ini bertujuan untuk menjelaskan bagaimana pengaruh kejahatan cyber transnasional terhadap strategi cyber defense Indonesia. Dalam penelitian ini juga mencoba menjelaskan strategi pemerintah Indonesia dalam menanggapi kejahatan kader lintas negara. Tingkat analisis penelitian ini adalah negara sebagai aktor internasional. Penelitian ini menggunakan perspektif realis dan menggunakan teori keamanan untuk menjelaskan masalah dalam kejahatan cyber ini. Penelitian ini merupakan penelitian kualitatif. Teknik pengumpulan data penelitian ini adalah studi kepustakaan. Hasil dari penelitian ini adalah pemerintah Indonesia memiliki strategi untuk mengatasi pengaruh kejahatan cyber transnasional. Strategi Indonesia adalah kebijakan keamanan pertahanan dunia maya nasional.

Kata Kunci: kejahatan cyber, strategi indonesia, transnasional, kebijakan, keamanan

PENDAHULUAN

Perkembangan teknologi informasi yang demikian pesatnya haruslah di antisipasi dengan hukum yang mengaturnya dimana kepolisian merupakan lembaga aparat penegak hukum yang memegang peranan penting di dalam penegakan hukum. Sebab tanpa adanya hukum yang mengatur dan lembaga yang menegakkan maka dapat menimbulkan kekacauan didalam perkembangannya. Dampak negatif tersebut menimbulkan suatu kejahatan yang dikenal dengan nama *Cybercrime* yang tentunya harus diantisipasi dan ditanggulangi.[1]

Negara Indonesia merupakan negara terbesar di kawasan Asia Tenggara yang memiliki potensi ekonomi serta politik kawasan regional. Tentu saja masalah kejahatan siber menjadi sebuah masalah serius seiring banyaknya akses dalam bidang ekonomi, politik, pertahanan negara melalui jaringan sistem internet, sehingga hal ini menimbulkan masalah yang serius di terutama dalam keamanan akses data tersebut. Tidak hanya di negara Indonesia tetapi negara-negara lain juga memiliki masalah yang sama yaitu *cybercrim*e ini. Keamanan siber adalah kebutuhan nyata dan mendesak karena pengaruhnya berpotensi merusak atau mengganggu kehidupan, negara, dan bahkan seluruh dunia.

Direktur Korea Internet & Security Agency (KISA) Aaron Wonki Chung membeberkan kelemahan Indonesia dalam menghadapi serangan digital atau *cyber attack*. Berbicara dalam acara Joint Seminar Korean-Indonesian *on Cybersecurity* di Kantor Kementerian Koodinator Bidang Politik, Hukum, dan Keamanan, Aaron menyebutkan salah satu kelemahan tersebut adalah belum terintegrasinya sistem pertahanan siber.[2] Aaron melanjutkan saat ini para peretas telah memiliki kemampuan yang cukup untuk membuat kerusakan

[1] Kombes (Pol) Drs. Petrus Reinhard Golose, M.M, Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia oleh POLRI, 2006, *Buletin Hukum Perbankan dan Kebanksentralan*, Volume 4 Nomor 2, hal. 32-34.

[2] Rappler *News*, "*Korea Beberkan Kelemahan Pertahanan digital Indonesia*" Diakses dalam https://www.rappler.com/indonesia/berita/sains-dan-tekno/155592-korea-beberkan-kelemahan-pertahanan-digital-indonesia pada tanggal 8 Nopember 2017.

digital secara masif, karena itu perlu ada sistem pengamanan yang terintegrasi antar instansi pemerintah.

Indonesia berada di peringkat 13 dalam daftar indeks keamanan siber *global International Telecommunication Union* (ITU) dan ABI *Research* yang meliputi 193 negara di dunia. Wakil Asia yang masuk dalam peringkat lima terbaik dunia hanya Malaysia, yang menduduki peringkat ketiga bersama Australia atau hanya satu peringkat di bawah Amerika dan Kanada. Ada lima komponen utama yang dinilai dalam indeks ini yaitu ukuran legal, ukuran teknis, ukuran kelembagaan, peningkatan kapasitas, dan kerja sama. Di Indonesia, ID-SIRTII juga merilis laporan tahunan keamanan siber dalam acara *National Security Days* di Bandung pada November 2014. Menurut laporan tahunan ID-SIRTII (*Indonesia Security Incident Response Team on Internet Infrastructure/CoordinationCenter*) tersebut, Indonesia yang mendapat serangan siber lebih dari 42 juta sepanjang 2014 dan berisiko besar terkena dampak keamanan siber yang lemah.[3]

Kasus serangan siber selanjutnya seperti beberapa tahun yang lalu sejumlah pemberitaan yang menyangkut masalah penyadapan yang dilakukan pihak asing kembali mengemuka, setelah sebelumnya pada akhir bulan Oktober 2013 Indonesia dikejutkan dengan sejumlah pemberitaan tentang tindakan Australia yang terbukti telah melakukan penyadapan terhadap sejumlah pejabat tinggi Pemerintah Indonesia, termasuk penyadapan terhadap Presiden Susilo Bambang Yudhoyono. Nama Indonesia kembali muncul dalam pemberitaan terkait skandal penyadapan oleh Badan Keamanan Nasional Amerika Serikat atau NSA (*No Such Agency*). Isu tersebut dimuat dalam harian *The New York Time* yang dilansir tanggal 15 Pebruari 2014, yang dibocorkan oleh mantan kontraktor NSA Edward J Snowden.[4]

Informasi yang didapat NSA ini berasal dari Direktorat Sinyal Australia atau ASD (*Australian Signals Directorate*). ASD awalnya, memberitahu NSA bahwa mereka melakukan pemantauan komunikasi termasuk antara pejabat Indonesia dengan firma hukum di Amerika Serikat. Disebut dalam dokumen itu, ASD bersedia berbagi informasi dengan NSA. Terhadap masalah tersebut, Menteri Luar Negeri Marty Natalegawa pada tanggal 17 Pebruari 2014 telah menyatakan sikap kekecewaan Indonesia terhadap Australia.[5] Dari penjelasan kasus-kasus di atas sudah jelas bahwa Indonesia merupakan salah satu negara yang sangat rawan terhadap serangan siber terutama dari luar wilayah hal ini sangat diperlukan penanganan yang luar biasa dari pihak pemerintah.

Sebagai negara berkembang, Indonesia sedikit tertinggal dalam mengikuti perkembangan teknologi informasi, sebagai hasil dari strategi pengembangan teknologi yang tidak tepat yang mengabaikan penelitian ilmiah dan teknologi. Akibatnya, alih teknologi dari negara industri maju tidak diikuti oleh penguasaan teknologi itu sendiri yang mengubah Indonesia menjadi negara berbasis teknologi.[6] Pertahanan nasional negara-negara di dunia saat ini sudah mengalami pergeseran pandangan yang dahulu lebih pada militer menuju ke masalah pertahanan negara non-militer yang sebenarnya jauh lebih berbahaya di era modern saat ini. Ini merupakan indikator yang kuat bahwa pemerintah Indonesia harus selalu mengikuti perkembangan teknologi yang cepat dan mengantisipasi dampak-dampak bahaya untuk pertahanan nasional.

METODE

Model analisis yang digunakan dalam penelitian ini lebih mengarah pada penggunaan model penelitian kualitatif-deskriptif. Model penelitian kualitatif adalah strategi penelitian yang menekankan kedekatan dengan data, partisipasi dan pengalaman. Penelitian ini

[3] Antara *News*, "*Indonesia di peringkat 13 dunia dalam keamanan siber*" diakses dalam http://www.antaranews.com/berita/468748/indonesia-di-peringkat-13-dunia-dalam-keamanan-siber pada tanggal 09 Nopember 2017.

[4] Gatot S. Dewa Broto, Kepala Pusat Informasi dan Humas Kementerian Kominfo "*Penyadapan Australia terhadap Indonesia*" Diakses dalam http://postel. go.id/berita-tindak-lanjut-kominfo-terhadap-masalah-penyadapan-26-2134 pada 4 Nopember 2017.

[5] *Ibid.*

[6] *Ibid.*

menekankan pengumpulan fakta dan identifikasi data. Komponen metode dalam penelitian ini adalah mendeskripsi, menganalisa, dan menafsirkan temuan dalam istilah yang jelas dan tepat.

HASIL DAN PEMBAHASAN

Penelitian ini menggunakan teori sekuritisasi (*securitization*) yang dikemukakan oleh Ole Waever. Dalam buku *On Security*, Ole Waever menyatakan bahwa: security sebagai "*speech act*". Dengan mengartikulasikan keamanan, pemerintah bergerak dari fakta-fakta yang sifatnya umum kemudian masuk dalam area yang sifatnya spesifik kemudian mengambil langkah-langkah apa pun sebagai bagian dari hak istimewanya untuk dapat menghentikannya.[7] Dilanjutkan dalam buku *Security: A New Framework of Analysis*, Buzan, Waever dan Jaap de Wilde mengemukakan: Keamanan adalah langkah yang dilakukan dengan melampaui aturan main secara umum dalam membingkai suatu isu apakah isu tersebut termasuk dalam ranah politik atau melampauinya.[8]

Sekuritisasi menurut Buzan, Waever dan Jaap de Wilde adalah sebuah bentuk ekstrem dari upaya politik. Setiap isu publik dapat dikategorikan dalam tiga jangkauan yang antara lain, *nonpoliticized* yang berarti pemerintah tidak menanggani permasalahan ini karena tidak termasuk dalam isu yang menyangkut kepentingan dan perdebatan dalam ranah publik. *Politicized*, yang berarti bahwa isu tersebut telah masuk pada ranah kebijakan publik yang membutuhkan campur tangan pemerintah dalam hal alokasi sumber daya, atau kebijakan tambahan. Selanjutnya, *to securitized*, yang berarti bahwa sebuah isu telah dianggap sebagai ancaman kemananan yang bersifat nyata, yang tentu saja membutuhkan tindakan yang darurat dimana penggunaan prosedur diatas prosedur politik biasa dianggap sah untuk dilakukan.[9]

Aktivitas Serangan Siber Trnasnasional Terhadap Indonesia

Indonesia menjadi sasaran penyadapan yang dilakukan oleh Amerika Serikat (AS). Penyadapan terhadap Indonesia dilakukan NSA (*National Security Agency*) Amerika bekerja sama dengan Direktorat Sandi Pertahanan (DSD) Australia. Sebagai contoh, NSA-AS meminta bantuan DSD Australia untuk mematai-matai Indonesia pada waktu Konferensi Perubahan Iklim PBB yang diadakan di Bali, tanggal 3–14 Desember 2007. Penyadapan kala itu dilakukan Amerika dan Australia untuk memantau struktur jaringan komunikasi keamanan Indonesia.[10]

Selain melakukan penyadapan pada waktu Konferensi Perubahan Iklim, DSD-Australia juga melakukan penyadapan terhadap komunikasi Presiden Susilo Bambang Yudhoyono (SBY) dan para pemimpin Indonesia lainnya. Alasan Australia membantu Amerika melakukan penyadapan adalah untuk memajukan kepentingan nasionalnya sendiri serta sebagai kontribusi terhadap aliansi dengan Amerika. Penyadapan yang dilakukan Australia telah berlangsung dalam berbagai bentuk selama 20 tahun sampai 30 tahun.

Pada tahun 2013 pemerintah Indonesia melalui Institut Teknologi Bandung (ITB) kembali membuat sebuah terobosan baru di bidang Ilmu Pengetahuan dan Teknologi (Iptek) dengan membangun fasilitas *Cyber Security* di kampus ITB Jatinangor. ITB menggandeng Pemerintah Korea Selatan, melalui institusi bernama Korea *International Cooperation Agency* (KOICA). KOICA ialah sebuah institusi yang membantu dalam mendiagnosis keamanan infrastruktur negara-negara yang bekerjasama dengan Korea Selatan, salah

---

[7] Ole Waever, *Securitization and Desecuritization* , dalam Ronnie D. Lipschutz (ed) *On Security*, New York: Columbia University Press, 1995, hal. 55.

[8] Barry Buzan, Ole Waever, Jaap de Wilde, *Security: A New Framework of Analysis*, London : Lynne Riener Publisher, 1998, hal. 23.

[9] *Ibid*, hal. 23.

[10] Lisbet, "*Sikap Indonesia Terhadap Isu Penyadapan Amerika Serikat dan Australia*", Pusat Pengkajian, Pengolahan Data dan Informasi (P3DI) Sekretariat Jenderal DPR RI, Vol. V, No. 21/I/P3DI/November, 2013, hal. 6.

satunya Indonesia berdasarkan tujuan untuk mendiagnosis fasilitas-fasilitas di Indonesia demi keselamatan masyarakat Indonesia terjaga dari kejahatan siber. Kerjasama ini di bawah pengawasan Kementerian Komunikasi dan Informatika Republik Indonesia.[11]

Selanjutnya kelompok teroris masa kini mengerti bahwa pembuat kebijakan di negara demokrasi Liberal tidak akan dan tidak bisa mengabaikan media serta opini publik. Kelompok teroris juga menyesuaikan metode dan pesan-pesan dengan teknologi berita. Selain itu, media massa juga dipakai sebagai alat untuk memperoleh dukungan massa seperti sarana untuk rekrutmen anggota, terutama dari kalangan terpelajar dan terdidik yang tidak puas dengan kebijakan-kebijakan pemerintah. Rekrutmen anggota akan semakin berhasil apabila kebijakan pemerintah menyebabkan kesenjangan ekonomi yang mencolok antara kelompok yang kaya dan miskin.

Akibat dari kejahatan dunia maya dapat lebih luas daripada tindak pidana konvensional, karena para pelaku tidak dibatasi oleh waktu dan geografis, oleh karena itu wilayah terjadinya tidak hanya secara lokal atau nasional tetapi juga transnasional dan internasional. Kejahatan dunia maya yang akhir-akhir ini sering dilakukan adalah *carding*. *Carding* atau yang bisa disebut juga *credit card fraud* (penipuan kartu kredit).

Kejatan Siber *Carding* atau kebocoran kartu kredit terjadi karena adanya data *Leakage* atau kebocoran data. Data *Leakage* adalah suatu pembocoran data rahasia yang dilakukan dengan cara menulis data rahasia tersebut ke dalam kode-kode tertentu sehingga data tersebut dapat dibawa keluar tanpa diketahui oleh pihak yang bertanggung jawab. Kasus *carding* di Indonesia bermunculan ketika terjadi.

Booming internet di era tahun 2000-an. Beberapa kota seperti Jakarta, Bandung dan Yogyakarta menjadi pusat-pusat *carder* dalam melancarkan aksi pencurian data kartu kredit. Aksi-aksi *cybercrime* ini mengakibatkan pada tahun 2004, transaksi *on-line* yang berasal dari IP (*Internet Protocol*) Indonesia diblokir oleh dunia internasional. Dari kasus-kasus *cyber-crime* khususnya *carding* tersebut yang benar-benar diproses di pengadilan di Indonesia dapat dihitung dengan jari. Sangat jarang muncul ke media massa para *carder* dijerat dengan hukum yang setimpal dengan perbuatannya.[12]

Seperti yang diberitakan di beberapa media baik di dalam ataupun luar negeri, telah terjadi fenomena serangan siber di beberapa negara, termasuk Indonesia. Direktur Jenderal Aplikasi Informatika, Semuel A. Pangerapan seperti dikutip dari laman kominfo.go.id menyampaikan, serangan siber ini bersifat tersebar dan masif serta menyerang *critical resource* (sumber daya sangat penting), maka serangan ini bisa dikategorikan teroris siber. Di Indonesia serangan ditujukan ke dua rumah sakit di Jakarta.[13]

Serangan siber yang menyerang Indonesia berjenis *ransomware*. *Ransomware* adalah sebuah jenis *malicious software* atau *malware* yang menyerang komputer korban dengan cara mengunci komputer korban atau meng-*encrypt* semua file yang ada sehingga tidak bisa diakses kembali. Serangan sebuah virus berjenis *Ransomware* yang orang-orang memanggilnya dengan *sebutan WannaCry*. Nama *WannaCry* merupakan singkatan dari nama aslinya yang bernama *Wanna Decryptor*.[14]

---

[11] Elin Konstantia Novel,"*Kerjasama Indonesia-Korea Selatan Dalam Mengimplementasikan Keamanan Cyber Dengan Studi Kasus Cyberporn"*, Jurnal FISIP HI: Universitas Riau, Vol. 5, 2018.

[12] Leo T. Panjaitan,"*Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik no.11 Tahun 2008"*, Jurnal Telekomunikasi dan Komputer, vol.3, no.1, 2012, hal. 13.

[13] Media Indonesia *News*, "*Virus WannaCry juga Serang Indonesia*", diakses dalam http://media indonesia.com/read/detail/104581-virus-wannacry-juga-serang-indonesia pada tanggal 27 April 2018.

[14] Codepolitan *News*, "*Heboh Serangan Virus WannaCry Di Indonesia"*, diakses dalam https://www.codepolitan.com/heboh-serangan-virus-wannacry-di-indonesia-591950516b362 pada tanggal 27 April 2018.

Aktor Kebijakan Pertahanan Siber Indonesia

Dalam proses strategi keamanan tentu akan ada aktor utama yang melakukan propses tersebut. Aktor strategi keamanan dalam penelitian ini berkaitan dengan lembaga-lembaga suatu institusi negara. Indonesia memiliki banyak lembaga yang menjadi aktor utama dalam pertahanan siber negara dan tentunya lembaga itu yang berkaitan masalah siber. Aktor utama dalam pertahanan keamanan ini sangat penting karena dengan adanya aktor tersebut proses pertahanan keamanan suatu masalah akan terwujud dan akan memberi dampak bagi kepentingan negara.

Presiden Republik Indonesia, Joko Widodo pada tanggal 19 Mei 2017 telah menandatangani Peraturan Presiden (Perpes) Nomor 53 tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN). BSSN merupakan lembaga pemerintah non kementerian yang berada di bawah dan bertangung jawab kepada Presiden melalui menteri yang menyelenggarakan koordinasi, sinkronisasi, dan pengendalian penyelengaraan pemerintahan di bidang politik, hukum, dan keamanan.[15]

Kementerian Pertahanan menjadi salah satu aktor sekuritisasi sistem pertahanan siber Indonesia karena memiliki peran dalam terwujudnya proses sekuritisasi siber. Ancaman siber sudah termasuk ancaman yang nyata bagi kedaulatan negara. Salah satu ancaman bahaya siber lintas batas adalah adanya serangan virus dari luar negeri dan juga banyak sekali kasus-kasus penipuan dalam bisnis online lintas negara bahkan negara menjadi sasaran penyadapan pada kasus penyadapan oleh Australia terhadap banyak pejabat di lingkungan pemerintah Indonesia.

Dalam Buku Putih Pertahanan Indonesia pada tahun 2015, Menteri pertahanan saat itu Ryamizard Ryacudu memamandang bahwa Perkembangan lingkungan dan konteks strategis yang dinamis senantiasa membawa perubahan terhadap spektrum ancaman yang kompleks dan berimplikasi terhadap pertahanan negara. Kompleksitas ancaman digolongkan kedalam pola dan jenis ancaman yang multidimensional berupa ancaman militer, ancaman nonmiliter dan ancaman hibrida yang dapat dikatagorikan dalam bentuk ancaman nyata dan belum nyata. Dengan demikian, pertahanan negara kedepan memerlukan keterpaduan pertahanan militer dan pertahanan nirmiliter melalui usaha membangun kekuatan dan kemampuan pertahanan negara yang kuat dan disegani serta memiliki daya tangkal tinggi.

Kementerian Komunikasi dan Informatika Republik Indonesia (Kemkominfo RI) adalah kementerian dalam Pemerintah Indonesia yang membidangi urusan komunikasi dan informatika. Kementerian Komunikasi dan Informatika mempunyai tugas menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika untuk membantu Presiden dalam menyelenggarakan pemerintahan negara.

Pandangan urgensinya kondisi siber Indonesia disampaikan oleh Deputi Kepala Bidang Teknologi Informasi Energi dan Material Badan Pengkajian dan Penerapan Teknologi (TIEM BPPT), Hammam Riza menyatakan[16] pemerintah harus segera menerapkan pengamanan tingkat tinggi dalam pengamanan siber. Infrastuktur kritis itu harus memiliki tingkat keamanan yang tinggi, mampu menahan bahaya, dan bisa segera pulih jika mengalami serangan yang sifatnya merusak. Bahkan, Hammam menilai, penerapan teknologi keamanan siber sudah sangat mendesak. Dunia siber Indonesia dalam kondisi darurat untuk diterapkannya teknologi keamanan siber (*Cybersecurity*). Perlu penguatan terhadap keamanan infrastruktur informasi kritis.

Kementerian Luar Negeri RI melalui staf ahli bidang antar lembaga Salman Al Farisi pada tahun 2017 dalam acara pembahasan *Policy Paper* dengan teme "Diplomasi Siber

[15] Badan Siber dan Sandi Negara (BSSN), diakses dalam https://bssn.go.id/sejarah-pembentukan-bssn/ pada tanggal 12 Juli 2018.

[16] Kementerian Komunikasi dan Informatika RI, "*Dunia Siber Indonesia Dinilai Darurat*", diakses dalam https://www.kominfo.go.id/content/detail/7748/dunia-siber-indonesia-dinilai-darurat/0/sorotan_media pada tanggal 24 Agustus 2018.

Indonesia: Kini dan Nanti"[17] di Yogyakarta menyatakan bahwa teknologi informasi dan komunikasi yang terus berkembang mendorong pemerintah beradaptasi dengan kondisi global yang seakan tidak memiliki batas antar wilayah. Dengan kondisi ini, muncul masalah dan tantangan baru yang perlu dihadapi Indonesia. Kementerian Luar Negeri RI menegaskan perlunya diplomasi siber (*cyber diplomacy*) sebagai respon dari tantangan tersebut. Diplomasi siber juga ingin diarahkan untuk mendukung kepentingan nasional, terutama dalam mendukung pertumbuhan digitalisasi ekonomi dan memperkuat kapasitas nasional dalam menghadapi ancaman keamanan siber.

Badan Nasional Penanggulangan Terorisme (BNPT) adalah sebuah lembaga pemerintah nonkementerian (LPNK) yang melaksanakan tugas pemerintahan di bidang penanggulangan terorisme.[18] Dengan perkembangan era digital saat ini terorisme sudah termasuk dalam ranah kejahatan siber dikarenakan dalam proses perkembangan jaringan terorisme menggunakan teknologi dan informasi yang sangat memudahkan jaringan terorisme berkembang pesat.

Urgensinya kondisi terorisme di Indonesia melaui jaringan internet ini disampaikan oleh Delegasi Indonesia yang dipimpin oleh Kepala Badan Nasional Penanggulangan Terorisme (BNPT), Komjen Pol. Suhardi Alius M.H. saat menghadiri pertemuan ke-27 Komisi Pencegahan Kejahatan dan Peradilan Pidana PBB atau *Commission on Crime Prevention and Criminal Justice* (CCPCJ) yang diselenggarakan di Wina, Austria, pada tanggal 14 Mei 2018.[19]

TNI menilai uergensinya ancaman serangan siber dan hal ini disampaikan pada Panglima TNI Jenderal TNI Gatot Nurmantyo saat masih menjabat, beliau menyampaikan pada Sidang ke-4 *High Level Comitte* (HLC) Australia-Indonesia (Ausindo) di Canberra Australia pada tahun 2016 bahwa sangat perlu mewaspadai munculnya isu kejahatan siber sebagai tantangan baru yang membahayakan kehidupan bangsa dan negara di lingkungan strategis, baik pada tataran regional maupun global.[20]

Sebelumnya masa mantan Panglima TNI Moeldoko menjabat sudah melihat bahwa saat itu TNI sudah melihat urgensi memperkuat divisi siber yang bertugas menangkal serangan melalui dunia maya yang dapat terjadi kapan saja.[21] TNI memiliki peran strategis menjaga kedaulatan negara dari ancaman perang di dunia maya. Pasalnya ancaman siber memang nyata adanya, termasuk menjadi bagian dari perang proksi yang saat ini banyak didengungkan.

Wakil Kepala Kepolisian RI Komisaris Jenderal Syafruddin menyatakan bahwa Indonesia masuk dalam jajaran dua besar negara di dunia dengan kejahatan di dunia maya atau *cyber crime.* Syafruddin mengatakan bahwa data yang dihimpun pihaknya mendapati 90 juta kali serangan siber terjadi di Indonesia selama Januari hingga akhir Juni 2016. *Cyber crime* di Indonesia tertinggi ke dua di dunia setelah Jepang. Total serangan cyber ini ada 90 juta, pernyataan ini disampikan saat memberikan pidato di acara yang diselenggarakan oleh Badan Pengkajian dan Penerapan Teknologi (BPPT) di Jakarta pada 7 Juli 2017.[22]

Dalam menanggapi bahaya siber Polri

[17] Antara *News*, "Kemenlu: diplomasi siber mutlak diperlukan" diakses dalam https://jogja.antaranews. com/berita/351225/kemenlu-diplomasi-siber-mutlak-diperlukan pada tanggal 25 Agustus 2018.

[18] Peraturan Presiden Nomor 12 Tahun 2012 tentang Perubahan atas Peraturan Presiden Nomor 46 Tahun 2010 Tentang Badan Penanggulangan Terorisme.

[19] Badan Nasional Penanggulangan Terorisme, "*Indonesia Ajak Dunia Berantas Kejahatan Siber*", diakses dalam https://www.bnpt.go.id/indonesia-ajak-dunia-berantas-kejahatan-siber.html pada tanggal 25 Agustus 2018.

[20] Tentara Nasional Indonesia, "*Serangan Cyber Membahayakan Keutuhan Negara*", diakses dalam https://tniad.mil.id/2016/10/serangan-cyber-membahayakan-keutuhan-negara/ pada tanggal 20 Juli 2018.

[21] Sindo News, "*Bentuk Satuan Siber, TNI Siap Hadapi Serangan di Dunia Maya"*, diakses dalam https://nasional.sindonews.com/read/1248299/14/bentuk-satuan-siber-tni-siap-hadapi-serangan-di-dunia-maya-1507966324/13 pada tanggal 26 Agustus 2018.

[22] CNN Indonesia *News*, "*Polri: Indonesia Tertinggi Kedua Kejahatan Siber di Dunia"*, diakses dalam https://www.cnnindonesia.com/nasional/20180717140856-12-314780/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia pada tanggal 20 Juli 2018.

sangat memperhatikan penuh dikarenakan banyak sekali aktivitas siber lintas negara yang membahayakan atau menjadi ancaman keamanan masyarakat. Direktur Tindak Pidana (Dirtipid) Siber Bareskrim Brigjen Polri Fadil Imran mengatakan bahaya kejahatan siber sudah semakin memprihatinkan. Ancaman kejahatan siber pun setara dengan tindak pidana kejahatan lainnya karena membahayakan keamanan. Kejahatan siber membahayakan ekonomi infrastruktur kritis, perdagangan, dan keamanan pernyataan ini disampikan dalam sambutannya di *Business Transformation Through Tecnology* di Ritz Carlton, Jakarta pada 22 Nopember 2017.[23]

Badan Intelejen Negara melalui Jenderal Polisi Budi Gunawan sebagai kepala BIN menyatakan[24] bahwa tantangan serangan siber adalah nyata. Bahwa bahaya berbagai serangan siber ini telah menyancam keamanan nasional dan sendi-sendi dalam kehidupan berbangsa dan bernegara. Ancaman terhadap keamanan dalam negeri meliputi separatisme, terorisme, spionase, sabotase, kekerasan politik, konflik horizontal, perang informasi, perang siber dan ekonomi nasional.

Perkembangan ancaman siber sangat mengkhawatirkan dan seringkali tidak disadari bahwa sistem telah disusupi virus. Maka dari itu, ancaman siber perlu mendapat perhatian. Saat ini, penanganan ancaman siber cenderung lebih mengedepankan pendekatan teknologi. Hasil riset mengenai ancaman siber menunjukkan tren serangan meningkat dan kompleks, sehingga penanganan dari sisi teknologi saja belum cukup. Oleh karena itu, diperlukan penanganan dalam perspektif intelijen yang lebih komprehensif.

[23] Detik *News*, "*Polisi: Pidana Kejahatan Siber Sama Beratnya dengan Kasus Lain*", diakses dalam https://news.detik.com/berita/d-3739161/polisi-pidana-kejahatan-siber-sama-beratnya-dengan-kasus-lain pada tanggal 20 Juli 2018.

[24] Detik News, "*Tantangan Keamanan Siber di Hadapan Budi Gunawan*", diakses dalam https://news.detik.com/kolom/d-3329895/tantangan-keamanan-siber-di-hadapan-budi-gunawan pada tanggal 26 Agustus 2018.

SIMPULAN

Beberapa aktor sekuritisasi adalah Kementerian Luar Negeri, Badan Siber dan Sandi Negara, Badan Nasional Penggulangan Terorisme, Kementerian Pertahanan, Kementerian Teknologi dan Informatika, Badan Intelejen Negara, Dewan , Tentara Nasional Indonesia dan Kepolisian Republik Indonesia. Instansi-instansi ini bekerjasama dalam sistem yang membentuk suatu program keamanan siber Indonesia untuk menangkal segala bentuk kejahatan siber lintas negara yang jumlahnya dari tahun ke tahun semakin meningkat. Upaya dalam proses sekuritisasi tersebut adalah dengan menerbitkan Undangan-undanga tentang Informasi dan Telematika selanjutnya diterbitkannya Peraturan Presiden tentang pembentukan badan siber dan wewenangnya. Dalam segi faktor pendukung ada beberapa perekrutan sumber daya manusia bidang siber yang handal diiringi dengan penggunaan teknologi dalam negeri untuk jaringan sistem siber yang cukup bagus terutama produk vendor dalam negeri.

Kejahatan siber merupakan tanggung jawab segala lembaga atau instansi bahkan swasta. Pemerintah Indonesia berkomitmen menjaga kedaulatan negara dari berbagai ancaman kejahatan siber transnasional. Dengan berbagai penjelasan di atas sudah sangat jelas bahwa pemerintah Indonesia mengupayakan dan berusaha untuk mencegah terjadinya kerusakan yang diakibatkan kejahatan siber yang di tujukan baik kepada pemerintah atau kepada rakyat sipil. Kejahatan siber saat ini menjadi salah satu ancaman yang nyata yang perlu diantisipasi sejak dini mungkin guna meminimalisir segala kerusakan yang besar.

DAFTAR RUJUKAN

Ole Waever, *Securitization and Desecuritization*, dalam Ronnie D. Lipschutz (ed) *On Security*, New York: Columbia University Press, 1995.

Barry Buzan, Ole Waever, Jaap de Wilde, *Security: A New Framework of Analysis*, London : Lynne Riener Publisher, 1998.

Lisbet, "*Sikap Indonesia Terhadap Isu*

Penyadapan Amerika Serikat dan Australia", Pusat Pengkajian, Pengolahan Data dan Informasi (P3DI) Sekretariat Jenderal DPR RI, Vol. V, No. 21/I/P3DI/ November, 2013.

Elin Konstantia Novel,"*Kerjasama Indonesia-Korea Selatan Dalam Mengimplementasikan Keamanan Cyber Dengan Studi Kasus Cyberporn",* Jurnal FISIP HI:Universitas Riau, Vol. 5, 2018.

Leo T. Panjaitan,"*Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik no.11 Tahun 2008",* Jurnal Telekomunikasi dan Komputer, vol.3, no.1, 2012.

Petrus Reinhard Golose, *Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia* Oleh POLRI, 2006, Buletin Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2.

Rappler *News*, "*Korea Beberkan Kelemahan Pertahanan digital Indonesia*" Diakses dalam https://www.rappler.com/ indonesia/berita/sains-dan-tekno/ 155592-korea-beberkan-kelemahan-pertahanan-digital-indonesia pada tanggal 8 Nopember 2017.

Gatot S. Dewa Broto, Kepala Pusat Informasi dan Humas Kementerian Kominfo "*Penyadapan Australia terhadap Indonesia*" Diakses dalam http:// postel.go.id/berita-tindak-lanjut-kominfo-terhadap-masalah-penyadapan-26-2134 pada 4 Nopember 2017.