PERAN KEAMANAN SIBER DALAM MENGATASI KONTEN NEGATIF GUNA MEWUJUDKAN KETAHANAN INFORMASI NASIONAL

THE ROLE OF CYBER SECURITY IN OVERCOME NEGATIVE CONTENTS TO REALIZE NATIONAL INFORMATION RESILIENCE

Lauder Siagian[1], Arief Budiarto[2], Simatupang[3]
Prodi Strategi Pertahanan Udara Universitas Pertahanan
(pakkrt@gmail.com, ariefbimbing.unhan@gmail.com,
tupang2007@yahoo.com)

Abstrak -- Latar belakang perkembangan teknologi informasi dan komunikasi telah menjadikan dunia siber sebagai peluang terhadap seluruh aspek lini kehidupan manusia. Pada sisi lain perkembangan teknologi informasi/siber tersebut telah dijadikan media produksi dan penyebaran konten negatif seperti hoax, ujaran kebencian, penipuan, SARA, dan lain sebagainya. Tahun 2017 Kemenkominfo RI mencatat Jumlah konten negatif berdasarkan aduan masyarakat mencapai 51.456 konten. Masifnya penyebaran konten negatif di internet, selain sebagai serangan psikologis terhadap masyarakat luas, juga berpotensi tinggi sebagai phising untuk menyebarkan mallware yang mengancam integritas, kerahasiaan dan ketersediaan informasi serta keamanan infrastruktur. Oleh karena itu konten negatif di internet dikategorikan sebagai serangan siber (cyber attack) dan kejahatan siber (cyber crime) yang berdampak menimbulkan instabilitas ketahanan informasi nasional. Cyber Security berperan sebagai backbone dalam mengatasi konten negatif. Penelitian ini menggunakan metode kualitatif dengan pembahasan menggunakan pendekatan teori cyber security dan teori peran (role play theory). Hasil penelitian menunjukkan bahwa penyelenggaraan cyber security oleh Dirjen Aptika Kemenkominfo RI dan lembaga lain seperti Kemhan dan Pusinfolahta TNI telah dapat menjadi fundasi penyelenggaraan cyber security atau keamanan informasi tetapi belum sepenuhnya dapat mengatasi serangan siber konten negatif saat ini dan ancaman di masa yang akan datang disebabkan tingginya ketergantungan terhadap respon, mekanisme dan policy penyedia platform dan faktor lainnya. Disimpulkan bahwa konten negatif merupakan bagian dari serangan siber yang mengancam instabilitas ketahanan informasi nasional dan cyber security memiliki peran sebagai kebijakan, penguasaan teknologi informasi dan shok terapi dalam mengatasi konten negatif.
Kata kunci: Cybersecurity, Cybercrime, Serangan, Kandungan, Blokir

Abstrack - The background of the development of information and communication technology has made cyber world as an opportunity to all aspects of the human life line. On the other hand the development of information technology / siber has been used as media production and dissemination of negative content such as hoaxes, hate speech, fraud, racial intolerance, and so forth. Year 2017 Kemenkominfo RI recorded the amount of negative content based on complaints reached 51,456 content. The massive spread of negative content on the internet, as well as

[1] Lauder Siagian adalah Mahasiswa Magister Prodi SPU Universitas Pertahanan
[2] Dr. Arief Budiarto DESS adalah Dosen Tetap Universitas Pertahanan
[3] St. H.Simatupang, M.Si(Han) adalah Dosen Tetap Universitas Pertahanan

psychological attacks on the wider community, is also potentially high as a phishing to spread mallware that threatens integrity, secrecy and availability of information and security of infrastructure. Therefore, negative content on the internet is categorized as cyber attack and cyber crime, which has an impact on the instability of national information security. Cyber Security acts as a backbone in overcoming negative content. This research uses qualitative method with discussion using cyber security theory approach and role theory (role play theory). The results showed that the implementation of cyber security by the Directorate General of Aptika Kemenkominfo RI and other institutions such as Kemhan and Pusinfolahta TNI has been able to be the foundation of cyber security or information security but has not fully overcome the cyber attacks of current negative content and threats in the future due to the high dependence on platform responses, mechanisms and policy providers and other factors. It was concluded that negative content is part of cyber attack that threaten the instability of national information security and cyber security
Keywords: Cybersecurity, Cybercrime, Attack, Content, Blocking

Pendahuluan

Revolusi teknologi berlangsung dengan berkembangnya teknologi dan informasi yang begitu pesat. Hal tersebut telah membawa dampak yang besar berbagai aspek kehidupan seperti sosial budaya, ekonomi, politik, keamanan dan aspek pertahanan. Teknologi cyber atau yang lebih dikenal dengan TIK (Teknologi Informasi dan Komunikasi) membawa peluang yang besar sebagai backbone penggerak di berbagai bidang strategis. Bidang ekonomi digital/cyber berperan menggantikan transaksi manual yang dikenal dengan ecommerce, internet marketing dan internet banking (perbankan). Teknologi dan informasi menjadi *backbone* dalam kompetisi dalam kehidupan manusia modern. Saat ini, di masa depan. manusia memasuki pada era peradaban informasi. Peradaban informasi juga menciptakan perilaku manusia sebagai insan informasi. Umat manusia secara cepat menerima, mengelola, menyimpan, mengambil kembali dan mendistribusikan/mendiseminasi nformasi kepada sesama manusia. Bukan hanya slogan lagi yang menyatakan bahwa "siapa yang menguasai informasi maka dia akan menguasai dunia", hal tersebut sudah menjadi hukum yang nyata. Semakin memadainya ketersediaan informasi yang akurat akan semakin menentukan kualitas suatu keputusan. Informasi sudah dianggap sebagai "power" yang diartikan sebagai "kekuatan" dan "kekuasaan" yang sangat menentukan nasib manusia itu sendiri .

Perkembangan pesat pengguna internet juga terjadi di Indonesia. Merujuk kepada data statistik APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) bahwa pengguna internet di Indonesia tahun 2011 terdiri dari 55 juta orang, 2012 terdiri dari 63 Juta jiwa, 2013 terdiri dari 71,19 Juta jiwa, 2014 terdiri dari 107 Juta jiwa dan tahun 2015 berjumlah 139 Juta jiwa.[4] Hal tersebut menunjukkan pengguna internet di Indonesia berkembang pesat.

Dengan demikian, teknologi informasi menjadi media yang efektif untuk mempengaruhi alam pikir masyarakat luas dalam rangka membentuk opini yang positif/konstruktif. Disisi lain, teknologi informasi juga menjadi ancaman terhadap instabilitas kehidupan sosial masyarakat, berbangsa dan bernegara bilamana pemanfaatan pengetahuan dan teknologi informasi dijadikan untuk menyebarkan pemberitaan dengan konten negatif atau bersifat destruktif. Penyebaran informasi konten negatif melalui media teknologi informasi (internet) dengan berbagai aplikasi media sosial, media *online* dan berbagai aplikasi berbasis internet lainnya cenderung dilatarbelakangi oleh berbagai kepentingan seperti persaingan pribadi/individu, bisnis (motiv ekonomi) hingga politik.

Penyebaran konten negatif seperti berita bohong (hoax), hujatan, propagan dan agitasi telah dijadikan untuk mengganggu stabilitas keamanan, politik dan existensi negara baik dari dalam maupun luar negeri. Penyebaran konten negatif dengan motif politik masuk dalam ranah perang informasi *(information war/cyber war)*. Sehingga tindakan ini sudah diluar konteks kejahatan biasa *(cyber crime)*. Penggunaan teknologi informasi berkonten negatif seperti ini pada dasarnya telah menjadi media penyelenggaraan perang berdimensi asimetris (*asymmetric war)* dengan menggelar serangan *proxy war* (perang yang mempergunakan pihak ketiga).

Metode Penelitian

Penulisan tesis ini menggunakan metode penelitian kualitatif dengan pendekatan kepustakaan dan berdasarkan teori-teori dalam memahami peran cyber security guna mengatasi informasi konten negatif dalam mewujudkan ketahanan informasi nasional. Dengan metode penelitian ini

[4] APJII, 2015

diharapkan menghasilkan gagasan sebagai outcome pengolahan dan analisis data dengan menitik beratkan aspek kualitas sumber data. Tokoh peneliti Arief Furchan (1992) dalam bukunya Pengantar Metode Penelitian Kualitatif bahwa metode kualitatif ialah proses penelitian yang menghasilkan data deskriptif, ucapan atau tulisan atau perilaku yang dapat diamati dari orang-orang itu sendiri[5].

Hasil dan Pembahasan

Gambaran Umum Penyelenggaraan Cyber Security

1. **Kementerian Komunikasi dan Informatika RI**

   Website resmi Kominfo RI dijelaskan tentang sejarah singkat bahwa Kementerian Komunikasi dan Informatika (sebelumnya bernama "Departemen Penerangan" (1945-1999), "Kementerian Negara Komunikasi dan Informasi" (2001-2005), dan Departemen Komunikasi dan Informatika (2005-2009), disingkat Depkominfo) adalah Departemen Kementerian dalam Pemerintah Indonesia yang membidangi urusan komunikasi dan informatika. Kementerian Kominfo dipimpin oleh seorang Menteri Komunikasi dan Informatika (Menkominfo) yang sejak tanggal 27 Oktober 2014 dijabat oleh Rudiantara[6]

2. **Puskom Kemhan RI**

   Sesuai dengan Peraturan Menteri Pertahanan Republik Indonesia Nomor 58 Tahun 2014 Puskom Kemhan RI atau Pusat Komunikasi Publik adalah unsur pendukung pelaksana tugas dan fungsi pertahanan berada dibawah dan bertanggung jawab kepada Menteri.

3. **Pusinfolahta Mabes TNI**

   Website resmi Pusat Informasi Dan Pengolahan Data (Pusinfolahta) TNI dengan URL http://pusinfolahtatni.mil.id/tugas-dan-fungsi/ dijelaskan bahwa Pusat Informasi dan Pengolahan Data TNI (Pusinfolahta TNI) adalah jajaran yang berada dibawah dan bertanggungjawab langsung kepada Panglima TNI, sebagai Badan Pelaksana Pusat di tingkat Mabes TNI berdasarkan Keputusan Panglima TNI Nomor Kep/7/XII/2006 tanggal 5 Desember 2006.

[5] Furchan, A. (1992). Pengantar metode penelitian kualitatif.

[6] https://kominfo.go.id/profil

4. **Badan Siber dan Sandi Negara (BSSN**)

   Badan Siber dan Sandi Negara (BSSN) adalah badan pemerintah bidang Keamanan Informasi dan persandian dengan bersinergi dengan pemangku kepentingan baik institusi pemerintah maupun (private sector) swasta untuk ikut serta mewujudkan keamanan nasionalyang dipimpin oleh Kepala Badan BSSN yang dalam pelaksanaan tugasnya berada di bawah langsung Presiden Republik Indonesia.[7]

Analisis Data Dan Hasil Penelitian

Cyber Security

a. **Perlindungan Terhadap Serangan/Kejahatan Siber (Cyber Attack/Cyber Crime)**

   Paling mendasar pengertian dari cyber securiti adalah ditilik dari entimologi. Cyber security berasal dari bahasa inggris cyber dan security. Cyber berarti dunia maya atau dunia internet atau teknologi informasi (IT). Security berarti keamanan. Sehingga pengertian sederhada dari cyber security adalah keamanan cyber. Cyber security atau keamanan siber berfunsi atau berperan untuk mengatasi, mendeteksi, menemukan, menangkal ataupun meminimalisasi tingkat resiko terjadinya gangguan, ancaman (cyber threat) dan serangan siber (cyber attack) serta seluruh aktifitas teknologi siber yang mengancam keamanan seluruh komponen sistem siber itu sendiri yang meliputi hardware, software, data/informasi maupun infrastruktur. Merujuk kepada Konvensi cybercrime yang ditulis dalam buku Cybercrime Legislation dijelaskan bahwa yang menjadi sasaran dari aktifitas kejahatan cyber (cyber crime) adalah sistem keamanan siber.[8] Salah satu aktifitas cyber crime adalah terkait dengan konten negatif.

   1) pelanggaran terhadap kerahasiaan, integritas dan ketersediaan data dan sistem komputer (offences against the confidentiality, integrity and availability of computer data and systems);
   2) pelanggaran terkait dengan komputer (computer-related offences);
   3) pelanggaran terkait dengan konten atau konten negatif (content-related offences) ;and

[7] https://bssn.go.id/tugas-dan-fungsi-bssn/

[8] Gercke, M. (2010). Challenges in developing a legal response to terrorist use of the Internet. Gábor IKLÓDY, 37.

4) pelanggaran hakcipta (copyright-related offences)

b. Komponen Utama Cyber Security

Dengan memahami bahwa cyber security merupakan sistem yang berperan untuk melindungi informasi sistem dari gangguan dan serangan siber (cyber attack) atau segala aktifitas kejahatan siber (cybercrime), maka cyber security memiliki 3 (tiga) komponen utama. Komponen cyber security adalah model yang dirancang untuk memandu kebijakan keamanan informasi dalam sebuah organisasi sebagai sasaran penyelenggaraan cyber security itu sendiri, yaitu:

1) Confidentiality(kerahasiaan);
2) Integrity (integritas); and
3) Availability (ketersediaan).

c. Pengamanan Infrastruktur Informasi Kritis (Critical Information Infrastructure Security)

Infrastruktur informasi kritis merupakan bagian dari beberapa infrastruktur strategis/vital dalam suatu negara. Gambaran umum infrastruktur informasi kritis adalah infrastruktur yang menggabungkan antara jaringan telekomunikasi dan internet yang dipergunakan oleh masyarakat luas. Aspek keamanan Infrastruktur informasi kritis merupakan hal yang sangat penting. Terganggunya infrastruktur kritis akan berdampak fatal terganggunya dan atau lumpuhnya sektor strategis lainnya (ekonomi, pertahanan dan keamanan, energi d.l.l). Infrastruktur teknologi informasi menjadi tulang punggung berjalannya informasi berbagai lini politik, ekonomi, sosial, budaya, pertahanan dan keamanan meningkatkan potensi ancaman / gangguan pada sistem teknologi internet (Su, X., 2006). Keamanan Infrastruktur Informasi Kritis Nasional merupakan hal mutlak yang Untuk diselenggarakan guna efektivitas keandalan, ketersediaan dan integritas jaringan informasi, dalam tataran nasional dan internasional/global (Henderson, 2007).[9]

1) Kebijakan Strategis Infrastruktur Kritis di Indonesia

Pada buku Pedoman Pertahanan Siber yang disusun oleh Kementerian Pertahanan Republik

[9] Henderson, L. (2007). Theorizing a multiple cultures instructional design model for e-learning and e-teaching.

Indonesia, 2014, disebutkan bahwa Infrastruktur kritis adalah aset, sistem, maupun jaringan, berbentuk fisik maupun virtual yang sangat vital, dimana gangguan terhadapnya berpotensi mengancam keamanan, kestabilan perekonomian nasional, keselamatan dan kesehatan masyarakat atau gabungan diantaranya.

Indonesia telah mendefinisikan arti pentingnya infrastruktur kritis secara global, namun belum memiliki ketetapan dalam tataran nasional strategis atau perundang-undangan yang menetapkan bidang-bidang yang dikalsifikasikan sebagai objek dari infrastruktur kritis nasional.

Perlindungan terhadap Infrastruktur Informasi Kritis nasional atau critical information infrastructure protection (CIIP) oleh negara maju seperti Amerika telah ditetapkan sebagai kebijakan nasional yang melibatkan institusi pemerintah dan swata dalam suatu kordinasi nasional. Implementasi CIIP dibentuk dalam suatu sistem dan organisasi/kelembagaan yang profesional dan komprehensif. CIIP dibangun dengan Empat Pilar Model, yaitu:

1) Pencegahan dan Peringatan Dini
2) Deteksi
3) Reaksi; dan
4) Manajemen Krisis.

2. Infrastruktur Kritis Nasional Amerika

Amerika sebagai salah satu negara maju, telah menetapkan 16 sektor infrastruktur kritis yang bersifat vital terhadap kepentingan nasional Amerika.[10] Enam belas infrastruktur kritis yaitu:

a) Chemical Sector
b) Communications Sector
c) Dams Sector
d) Emergency Services Sector
e) Financial Services Sector
f) Government Facilities Sector
g) Information Technology Sector
h) Transportation Systems Sector
i) Commercial Facilities Sector
j) Critical Manufacturing Sector
k) Defence Industrial Base Sector
l) Energy Sector
m) Food and Agriculture Sector

[10] Dunn, M. (2005). The socio-political dimensions of critical information infrastructure protection (CIIP). International Journal of Critical Infrastructures, 1(2-3), 258-268.

n) Healthcare and Public Health Sector
o) Nuclear Reactors, Materials, and Waste Sector
p) Water and Wastewater Systems Sector

Konten negatif

1. **Konten Negatif Sebagai Serangan Siber (Cyber Attack)**

   Internet dan teknologinya semakin mendominasi peran dalam berbagai lini kehidupan baik di bidang pemerintahan, bisnis, ilmu pengetahuan, sosial dan bidang lainnya. Demikian halnya dalam arus lalu-lintas informasi dan komunikasi, internet telah menjadi tulang punggung (backbone). Internet sudah menghubungkan hampir seluruh manusia (netter) dan perangkat di seluruh penjuru dunia. Menurut catatan eMarketer, Pada tahun 2017 eMarketer memperkirakan pengguna internet (netter) Indonesia bakal mencapai 112 juta orang, sedangkan jumlah pengguna internet di seluruh dunia diproyeksikan bakal mencapai 3 miliar orang pada 2015 dan 2018, diperkirakanmencapai 3,6 miliar jiwa manusia. Data tersebut menjadi gambaran tentang internet sebagai peluang berbagai hal positif untuk manusia. Namun disamping penggunaan internet sebagai peluang juga mengandung potensi negatif bagi masyarakat internasional, regional dan nasional. Penggunaan teknologi internet untuk menyebarkan konten negatif seperti berita bohong (hoax), ujaran kebencian (hate speec), penipuan, isu SARA, pornograpi, teror dan sebagainya, sangat berpotensi tinggi dilakukan secara masif dan mudah oleh netter.

   Pemahaman tentang konten negatif secara umum dipahami sebagai suatu muatan berita atau informasi atau sebaran berupa gambar, video, suara maupun teks yang dapat dinilai bersifat negatif dipandang dari aspek etika, sosial, agama dan hukum. Menurut M. Salahuddien (praktisi dan konsultan Teknologi Informasi), saat ini menjabat sebagai Wakil Ketua ID-SIRTII (Indonesia Security Incident Response Team On Internet Infrastructure) dalam artikel Konsep Penyaringan Konten Porno di Internet (https://inet.detik.com) bahwa di Indonesia yang dimaksud dengan konten negatif di internet adalah yang mengandung perbuatan yang dilarang di dalam Undang Undang Nomor 11

Tahun 2008 Tentang Informasi dan Transaksi Elektronik.[11]

2. Jenis-jenis Konten Negatif

Secara kepada Konvensi cybercrime yang ditulis dalam buku *Cybercrime Legislation* dan UU RI nomor 11/2008 tentang ITE dirumuskan secara universal konten negatif meliputi seluruh aktifitas serangan dan kejahatan siber, sebagai berikut[12]:

1) Pornografi (Pornography)
2) SARA
3) Fitnah atau ujaran kebencian (hate speech)
4) Perjudian (Gambling)
5) Penipuan (Fraud Action)
6) Meresahkan Masyarakat (Disputing Society)
7) Terorisme/Radikalisme (Terrorism / Radicalism)
8) Perdagangan Produk dengan Aturan Khusus (Trade Products with Special Rules)
9) Pelanggaran HKI (Fraud Trade Products)
10) Kekerasan/Kekerasan Pada Anak (Children Violence) Pelanggaran Keamanan Informasi (Information Security Threat); dan
11) Aktifitas serangan atau kejahatan siber lainnya

3. Pelaku Konten Negatif

Konten negatif dapat di buat atau disebarluaskan oleh setiap pengguna internet (user generated). Konten negatif dapat dilakukan dengan memanfaatkan platform atau aplikasi media sosial seperti Bigo Live, Twitter, Instagram, Facebook dan lain-lain. Sedangkan pelaku konten negatif itu sendiri adalah terdiri dari tingkat individu/perorangan, kelompok dan bahkan oraganisasi yang lebih besar, dilakukan dengan memunculkan identitas asli, identitas akun palsu (fake account) dan atau tanpa identitas (anonymous). Penyebaran konten negatif bersifat masiv lebih berpeluang dilakukan oleh *buzze*r atau sistem robot (boot account) dimana akun didesain bekerja secara mesin atau otomatis.

Penyelenggaraan Cyber Security Mengatasi Konten negatif

Sebagaimana telah dijelaskan bahwa cyber securiti berperan untuk melindungi seluruh sistem baik informasi,

[11] Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

[12] Gercke, M. (2010). Challenges in developing a legal response to terrorist use of the Internet. Gábor IKLÓDY, 37.

software/harware maupun infrastruktus jaringan dari segala ancaman, serangan dan aktifitas kejahatan siber guna terlindunginya kerahasiaan (*confidentiality*), integritas (*Integrity*), dan ketersediaan (*availability*) informasi. Secara universal pendekatan dalam penyelenggaran keamanan informasi cyberspace yaitu pendekatan hukum, teknologi dan budaya.

1. Di Kemenkominfo RI

Penanganan konten negatif di internet dilakukan dengan kebijakan di semua lini dan diimplementasikan dengan metode pendekatan aspek hukum, teknologi dan budaya. Kebijakan dan pendekatan tersebut dijelaskan sebagai berikut:

a. Kebijakan

Menkominfo RI, Rudiantara telah menjelaskan kepada publik bahwa penanganan konten negatif.

1) **Kebijakan Disektor Hilir**

Kebijakan disektor hilir yaitu penanganan konten negatif berdasarkan Undang-undang Informasi dan Transaksi Elektronik (UU ITE Tahun 2008). Perwujudan kebijakan ini dilaksankan dengan tindakan pemblokiran konten, blokir website/aplikasi *platform* (Medol/Medsos) dan penindakan hukum. Disadarii bahwa langkah blokir yang dilakukan pemerintah belum tentu efeketif. Melakukan pemblokiran saja tidak akan efektif. Dengan demikian kebijakan sektor hulu yang bersifat prefentif juga sangat diperlukan.

2) **Kebijakan Di Sektor Hulu**

Kebijakan di sektor hulu adalah penaganan konten negatif dengan segala usaha dan upaya bagaimana mendorong, membangun dan menciptakan motivasi masyarakat pengguna internet *(netizen)* memberdayakan internet secara sehat dan bijaksana. Hal tersebut berarti suatu tindakan preventif untuk menciptakan motivasi netizen terhadap konten positif.

b. **Metode Pendekatan**

Kebijakan yang telah ditetapkan dalam penyelenggaran cyber securiti untuk mengatasi konten negatif, sebagai berikut:

1) Pendekatan Hukum

Konten-konten negatif yang ditemukan akan dianalisis untuk menilai dampak yang ditimbulkan oleh konten

tersebut untuk selanjutnya dilakukan proses hukum sesuai dengan aturan hukum terhadap seluruh pihak yang terlibat baik proses pembuatan maupun penyebarluasan konten kerjasama dengan Unit Cyber Crime Polri.

2) **Pendekatan Teknologi**

Pendekatan teknologi dalam mengatasi konten negatif di internet adalah dengan pemberdayaan teknologi secara umum dan secara khusus teknologi informasi dan komunikasi (TIK). Pemberdayaan teknologi khusus keamanan informasi didesain dengan program aplikasi atau tolls, hardware hingga infrastruktur untuk melakukan pengawasan (monitoring), deteksi, penyaringan (filtering) konten negatif. Negara-negara maju menjadikan mesin filtering sebagai alat sensor dan memblokir konten negatif. Dalam urusan keamanan internet, Tiongkok termasuk yang sangat peduli. Bagi negeri ini pemblokiran informasi kritis dari para aktivitas pro demokrasi sangat penting agar tidak merongrong kemapanan di dalam negeri.Tiongkok memiliki Great Firewall untuk menyaring konten internet. Sistem sensor internet skala besar ini membantu Tiongkok dalam memblokir konten "negatif" baik dari dalam negeri maupun luar negeri terkait dengan pemerintah di sana.

3) **Pendekatan Budaya**

Penanganan konten negatif dengan metode pendekatan budaya adalah penanganan bersifat prepentif atau mencegah. Dalam metode pendekatan budaya, tindakan difokuskan pada upaya menciptakan budaya mempergunakan siber atau internet secara sehat atau positif dengan mencegah muatan bersifat negatif. Memberikan literasi digital adalah salah satu teknis mendorong netizen untuk memerangi konten negatif.

c. Implementasi Penanganan Konten Negatif

Direktorat Jendral Aplikasi Informatika (Ditjen APTIKA) sebagai unit jajaran Kominfo RI yang

membidangi keamanan TIK, menyelenggarakan pengamanan informasi sesuai kebijakan yang ditetapkan.[13] Implementasi penanganan konten negatif dirumuskan dengan suatu mekanisme langkah prioritas meliputi Literasi Digital (Pendekatan Budaya), Sensors/Filtering (Pendekatan Teknologi) dan Penindakan (pendekatan Hukum)

1) **Pendekatan Budaya: Literasi Digital**

   Literasi digital di definisikan sebagai praktik berkomunikasi, berhubungan, berpikir dan 'menjadi' berhubungan dengan digital media. *"Practices of communicating, relating, thinking and 'being' associated with digital media"*.[14] Literasi digital merupakan penanganan pertama. Langkah ini adalah bertujuan untuk menciptakan kontrol sosial dan budaya yakni budaya internet positif dengan mendorong meningkatnya *level of literacy* dan kesadaran untuk tidak akses konten ilegal dan bijak dalam bermedsos semakin meningkat. saat ini *level of literacy* di Indonesia masih rendah dan harus digalakkan agar semakin meningkat. Level of literacy menimbulkan kesadaran *(netizen awarness)* untuk tidak mencari dan mengakses konten ilegal dan membentengi diri dan tidak menyebarkan informasi tidak terferifikasi seperti *hoax*, ujaran kebencian, provokasi dan konten negatif lainnya. Itu semua adakah kontrol sosial dan budaya.

2) **PendekatanTeknologi:Sensors/Filtering**

   Penanganan Pasif: *Crawling Manual*

   Adapun mekanisme penanganan konten negatif yang dilakukan atas dasar pengaduan tentang adanya konten negatif adalah pencarian konten negatif dengan sistem crawling, penyelidikan dan penindakan. Pencarian konten negatif dengan sisten

[13] Wawancara dengan Kepala Biro Humas Kominfo RI, Nor Izha.

[14] Jones, R. H., & Hafner, C. A. (2012). Understanding digital literacies: A practical introduction. Routledge.

crawling adalah proses menemukan konten didunia maya dengan memakai teknologi berupa tolls atau aplikasi khusus sebagai mesin pencari konten negatif, akan tetapi mesin akan berkerja berdasarkan input dari operator. Proses crowling dilakukan oleh Tim Trust+. Sistem di terapkan di router untuk memantau aliran data secara real-time dan melakukan tindakan.

Penaganan Aktif: *Crawling Otomatis AIS*

Penanganan konten negatif bersifat aktif adalah tindakan yang dilakukan secara terus menerus (bukan berdasarkan adanya pengaduan). Pencarian atau deteksi konten negatif dilakukan oleh teknologi seperti mesin pengais atau *crawling* yang bekerja secara sistem secara terus menerus dengan memasukkan *key word* indikator konten yang dicari. Mesin pencari konten negatif dinamakan *AIS* (berasal dari kata pengais) yang mampu bekerja secara cepat dan skala besar dan dioperasionalkan oleh unit *Cyber Drone 9.* Cyber Drone 9 terdiri dari dua ruang utama, *Security Operation Center (SOC Room)* dan *War Room.* Untuk SOC Room adalah dapur dari segala aktivitas pemantauan dan pengendalian terhadap konten negative[15]

2. Di Kemhan RI

Ancaman dan bahaya dari memproduksi dan menyebarluaskan konten negatif di dunia maya atau siber semakin dipahami secara luas. Perhatian akan masalah tersebut sebagai bagian dari keamanan informasi atau siber (cyber security) telah diimplementasikan walaupun masih dalam skala dan metode yang beragam. Puskom Kemhan RI memberikan perhatian yang cukup baik terkait dengan aliran informasi khususnya terkait dengan institusi Kemhan, Alutsista, Bela Negara, kerjasama pertahanan dan wilayah perbatasan.

a. Crawling

Melaksanakan monitoring pemberitaan media online terkait

[15] Kominfo, 2018

dengan Kementerian Pertahanan dan atau kebijakan pertahanan RI.

b. Analisis Sentimen negatif

Analisis sentimen negatif merupakan proses analisis terhadap seluruh informasi atau pemberitaan yang muncul di media online yang berhasil di deteksi oleh mesin atau tolls crawling.

c Publikasi

Mempublikasikan informasi yang akurat berupa tulisan/artikel dengan penyajian data yang baik untuk meluruskan opini atau sentimen negatif publik.

3. Pusinfolahta TNI

Pus-infolahta TNI saat ini menyelenggarakan upaya terkait dengan *cyber securiti* masih sebatas keamanan infrastruktur dan proteksi konten negatif secara terbatas

a. Keamanan Infrastruktur Jaringan.
b. Proteksi Konten Negatif.

4. Badan Siber dan Sandi Negara (BSSN)

Terkait dalam penanganan konten negatif, hingga saat ini BSSN tidak melaksanakan penganan konten negatif di dunia maya baik pada media online maupun media sosial. Kepala Badan Siber dan Sandi Negara (BSSN), Mayor Jenderal TNI (Purn) Djoko Setiadi menyatakan bahwa tugas BSSN saat ini menangani keamanan siber dan jaringan. Konten negatif di dunia siber/internet adalah ditangani oleh Kemenominfo Hal tersebut dirilis dalam website resmi Kemenkominfo (BSSN Hanya Tangani Keamanan Siber dan Jaringan.[16]

Pembahasan

Peran Cyber Securiti Mengatasi Konten Negatif

Hasil penelitian yang dilakukan terhadap peran cyber security dalam mengatasi konten negatif dunia maya atau cyber di Indonesia menunjukkan bahwa cyber security menjadi tulang punggung (backbound) dimana memiliki peran yang luas yang diwujudkan dalam suatu sistem pertahanan dan sebagai alat utama menghadapi serangan konten negatif di internet.

Berdasarkan pendekatan terhadap teori peran bahwa dimensi peran dapat berupa peran sebagai kebijakan, alat,

[16] https://kominfo.go.id/content/detail/12329/bssn-hanya-tangani-keamanan-siber-dan-jaringan/0/sorotan_media)

penyelesaian sengketa atau peran *shock terapy*.[17]

1. **Cyber Security sebagai kebijakan.** Dalam penanganan konten negatif dunia siber di Indonesia, pemerintah hadir melalui Dirjen Aptika Kominfo RI dengan suatu kebijakan yaitu penanganan hulu dan hilir.
2. **Cyber Security sebagai instrumen atau alat** Cyber Security sebagai umen mengatasi serangan siber konten negatif diimplementasikan dengan pemberdayaan teknologi aplikasi Nawala dan *crowling system.*
3. ***Cyber Securiti* sebagai *Shock Terapy*.** Tindakan pemlokiran dan filterisasi konten juga memberikan efek *shock terpy*
4. **Cyber Security sebagai Penyelesaian Sengketa**

Konten Negatif, Ancaman Terbesar Internet Indonesia Saat Ini Dan Masa Yang Akan Datang

Menurut hasil penelitian bahwa beberapa faktor utama yang menjadi pendorong berkembangnya konten negatif internet di Indonesia antara lain:

1. Pesatnya perkembangan pengguna internet *(netter)* di Indonesia
2. Pembangunan infrastruktur IT
3. Kurangnya literasi digital

Pada rapat koordinasi Kemenkominfo RI dengan Komisi I DPR pada tanggal 28 Nopember 2017 disampaikan bahwa periode Januari - Oktober 2017, tercatat 51.456 konten negatif di internet berdasarkan aduan masyarakat.[18]

Hasil penelitian menunjukkan bahwa tahun 2016, jumlah aduan yang diroses dan diajukan oleh Kominfo RI untuk dilakukan tindakan *take down* terhadap konten baru terlaksana 50 %, sedangkan tahun 2017 mengalami peningkatan hingga 55 %. Hal tersebut menunjukkan bahwa penanganan konten negatif belum mencapai titik optimal. Lebih dari itu, jumlah konten aduan yang belum ditindak lanjuti akan menjadi penyumbang terhadap ancaman tahun berikutnya.

Kesimpulan

Cyber security merupakan tulang punggung *(backbone)* dalam rangka mewujudkan suatu sistem ketahanan informasi yang tangguh dalam mengatasi ancaman/serangan siber yang senantiasa menjadikan sistem keamanan informasi menjadi sasaran. *cyber security* memiliki

[17] Biddle dan Thomas, 1966

[18] Dirilis oleh www.beritasatu.com

peran yang luas yaitu sebagai kebijakan, instrumen (alat utama) dan sebagi shok terapi. Penyelenggaraan *cyber security* di Indonesia telah diimplementasikan oleh Dirjen Aptika Kominfo RI dengan kebijakan hulu dan hilir yang diimplementasikan dengan metode pendekatan budaya, teknologi dan hukum. Peran cyber security belum mampu sepenuhnya diimplementasikan untuk mengatasi ancaman dan serangan konten negatif saat ini ditinjau dari beberapa peran yang dimiliki, sebagai berikut:

1) Kebijakan hilir yakni melakukan sonsor/filtering konten negatif dan pemblokiran Medsos/Medol sulit diterapkan dengan masifnya tindakan atau aksi resistensi netizen atau kelompok masyarakat terhadap kebijakan tersebut.
2) Penguasaan/kendali pemerintah terhadap infrastruktur TIK (infrastructure controlling) belum terwujud sehingga cyber security sebagai instrumen dengan pendekatan teknologi mesin crawling, dalam penerapannya baru mampu mengakomodir 50 % pengaduan konten negatif. Hal tersebut berdampak menciptakan tingkat ketergantungan yang tinggi terhadap respon ISP (internet service provider) dan policy penyedia flatform aplikasi serta waktu proses dan mekanisme yang relatif panjang.
3) Shok terapi, dilaksanakn dengan pendekatan penindakan hukum terhadap pelaku konten negatif belum sepenuhnya dapat diselesaikan dengan alur hukum positif yang cepat/tepat sehingga kurangnya pencapaian efek jera.

Konten negatif di dunia siber selain sebagai kejahatan siber (cyber crime) juga bagian dari serangan siber (cyber attack). Konten negatif berdampak langsung terhadap timbulnya berbagai misinformasi di masyarakat luas yang berdampak terhadap psikis dan perilaku, yakni timbulnya berbagai kondisi negatif diberbagai lini/ aspek kehidupan bermasyarakat dan bernegara (aspek psikologis, stabilitas keamanan, politik, ekonomi d.l.l). Aktifitas menghasilkan dan atau menyebarkan konten negatif di dunia siber dengan berbagai motifasi/latarbelakan, khususnya bidang politik akan mengancam kepentingan nasional yaitu stabilitas ketahanan nasional bidang informasi.

Referensi

Buku

Dunn, M. (2005). The socio-political dimensions of critical information infrastructure protection (CIIP). International Journal of Critical Infrastructures, 1(2-3), 258-268

Furchan, A. (1992). Pengantar metode penelitian kualitatif.

Henderson, L. (2007). Theorizing a multiple cultures instructional design model for e-learning and e-teaching.

Jones, R. H., & Hafner, C. A. (2012). Understanding digital literacies: A practical introduction. Routledge

Perundang-undangan

Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Artikel Online

Jumlah Pengguna Internet Indonesia" APJII,http://www.apjii.or.id/v2/index.php/read/page/halamandata/9/statistik.html#, dikutip dari website APJI, diakses 20 Februari 2018

ProfilKominfo,https://kominfo.go.id/profilhttps://bssn.go.id/tugas-dan-fungsi-bssn/, diakses 10 januari 2018

Kominfo, "BSSN Hanya Tangani Keamanan Siber dan Jaringan",https://kominfo.go.id/content/detail/12329/bssn-hanya tangani-keamanan-siber-dan-jaringan/0/sorotan_media,diakses 10 Januari 2018.