STRATEGI KEAMANAN SIBER KOMISI PEMILIHAN UMUM (KPU) PUSAT DALAM MENGHADAPI PEMILU 2019

THE CYBER SECURITY STRATEGY OF GENERAL ELECTIONS COMMISSION IN FACING THE GENERAL ELECTION 2019

M. Syadli Pratama[1], Fetri Miftach[2], Yusuf Ali[3]

Prodi Peperangan Asimetris Fakultas Strategi Pertahanan Universitas Pertahanan

(syadli.pratama@idu.ac.id)

Abstrak--Kajian ini menganalisa keamanan siber pada pelaksanaan Pemilu yang tengah menjadi sorotan saat ini. Banyaknya serangan siber yang dialami oleh KPU dalam penyelenggaraan pesta demokrasi sejak Pemilu 2014, ternyata tidak hanya sebatas ancaman peretasan terhadap infrastruktur, tetapi juga telah merambah ke ranah sosio kultural dengan pergeseran ke Pemilu 2.0 yang ditandai dengan semakin intensifnya peran sosial media sebagai medium opini publik. Peneliti menggunakan teori strategi sebagai grand theory oleh Carl Von Clauswitz dan konsep keamanan siber oleh Ghernaoutti untuk mengkaji dimensi keamanan siber. Metode penelitian ini menggunakan kualitatif dengan pendekatan fenomenologi. Hasil penelitian ini mengungkapkan bahwa strategi keamanan siber yang diimplementasikan oleh KPU Pusat dalam menghadapi Pemilu 2019 adalah melalui kerjasama dengan konsep *Triple Helix* yang melibatkan Pemerintah, Akademisi dan Swasta. Pengamanan siber dilakukan pada 4 (empat) dimensi melalui deteksi, proteksi dan prevensi terhadap ancaman dimulai dari aspek teknologi hingga ke manusianya. Kajian ini juga menyumbangkancara untuk menganalisa terkait peta ancaman Pemilu, jenis serangan, maupun metode kerjasama yang selama ini dilaksanakan oleh KPU dengan para *stakeholders* lainnya.
Kata kunci: strategi, keamanan siber, komisi pemilihan umum, triple helix

Abstract--*The study analyzes the the implementation of cyber security in the election which is currently become the spotlight. The number of cyber attacks experienced by the KPU in conducting a democratic party since the 2014 General Election was not only limited to the threat of hacking on infrastructure, but also penetration of the socio-cultural realm with a shifting to 2.0 elections marked by increasingly intensive social media role as a medium of public opinion. The researcher uses strategy theory as a grand theory by Carl Von Clauswitz and cyber security concepts by Ghernaoutti to examine cyber security dimensions. This research method uses qualitative phenomenological approaches. The results of this study reveals that the cyber security strategy implemented by the Central KPU in dealing with the 2019 Election is through Triple Helix cooperation concept involving the Government, Academics and the Private Sector. Cyber security is carried out on 4 (four) dimensions through detection, protection and prevention of threats starts from technology to human aspect. The study*

[1] M. Syadli Pratama, M. Han. Lulusan Program Pasca Sarjana Universitas Pertahanan, pada program peperangan Asimetris

[2] Fetri Miftach, Ph.D., C.Eng., MBCS Dosen Fakultas Strategi Pertahanan, Universitas Pertahanan

[3] Kolonel Cba. Dr. Yusuf Ali S.E., M.M Sesprodi Manajemen Pertahanan dan Dosen Fakultas Manajemen Pertahanan, Universitas Pertahanan

also contributes ways to analyze related maps of election threats, types of attacks, as well as methods of cooperation that has been carried out by KPU with other stakeholders.
Keywords: strategy, cyber security, general election commission, triple helix

Pendahuluan

Perkembangan globalisasi yang dipercepat oleh teknologi informasi berdampak pada arus informasi dan komunikasi yang mengalir secara luas tanpa mengenal batas ruang dan waktu. Globalisasi membentuk satu kesatuan masyarakat dunia yang terintegrasi[4] yang terbentuk melalui dua dimensi, yaitu dimensi ruang dan waktu, dimana dimensi ruang semakin dipersempit dan waktu yang semakin dipersingkat.[5] Jan Aart Scholte mendefinisikan globalisasi sebagai suatu proses transformasi lingkungan global sebagai kontinuitas dari situasi sebelumnya yang ditandai dengan ciri kemajuan teknologi dan informasi, menimbulkan interdepedensi, pengaburan terhadap batas-batas negara (*borderless state*).[6] Sehingga, dari beberapa definsi tersebut dapat disintesakan bahwa proses globalisasi dipercepat oleh kemajuan teknologi informasi yang memberikan dampak besar dan signifikan dalam konstelasi hubungan antar negara tanpa adanya batasan ruang dan waktu. Melihat dampak yang diakibatkan oleh teknologi informasi itu sendiri, banyak negara memandangnya sebagai suatu peluang yang dapat memberikan kontribusi positif bagi kesejahteraan masyarakatnya dan global, akan tetapi tak sedikit pula memandangnya sebagai suatu bentuk ancaman asimetris terhadap eksistensi mereka.

Ruang siber (*Cyberspace*) merupakan bidang jaringan komputer (termasuk para pengguna dibaliknya) dimana informasi disimpan, dibagikan dan dikomunikasikan secara *online*.[7] Ruang siber sendiri sebagai salah satu produk dari perkembangan teknologi informasi yang kini menjadi domain terbaru pada perang generasi ke-5 selain darat, laut, udara dan luar angkasa. Sebagai suatu domain baru, ruang siber menginterkoneksikan berbagai sistem terkomputerisasi melalui jaringan yang mendukung bekerjanya

[4] Albrow, Martin and Elizabeth King (eds). *Globalization, Knowledge and Society* (*London: Sage*, 1990), hlm 8
[5] Krisna. *Pengaruh Globalisasi Terhadap Pluralisme Kebudayaan Manusia di Negara Berkembang.* (Public Journal, 2005), hlm 72
[6] Scholte, J.A. *Globalization: A Critical Introduction.* (London: Palgrave McMillan, 2000), hlm. 7
[7] James A. Green. *Cyber Warfare A Multidisciplinary Analysis.* (Lanchester University: Routledge Studies in Conflict, Security and Technology.2015), hlm. 2

infrastruktur nasional yang kritis (*Critical National Infrastructure*) yang menjadi jantung kehidupan dari suatu negara.

Dengan segala efektifitas dan efisiensi yang ditawarkan dalam perkembangan dunia siber, maka terjadi konvergensi dan depedensi akan pemanfaatan dunia siber oleh banyak negara yang terus mengalami eskalasi signifikan dari tahun ke tahun dan tentunya hal ini membuka pintu ancaman yang beresiko tinggi terhadap keamanan nasional. Dengan alasan inilah mengapa ruang siber menjadi teater perang asimetris yang rentan terhadap berbagai ancaman yang tidak hanya berasal dari pihak internal atau eksternal, dan tidak hanya dilakukan oleh individu (*individuals*), kelompok (*non-state actors)*, bahkan oleh suatu negara (*state actors)* dengan tujuan keuntungan pribadi atau kelompok baik moneter, militer maupun suatu kepentingan politik.[8]

Pemilihan umum sebagai pilar demokrasi dalam penyelenggaraan pemerintahan suatu negara menjadi hal fundamental dan krusial. Sehingga, adanya gangguan pada pelaksanaan pemilu dapat berimbas pada kekacauan politik hingga instabilitas keamanan dalam negeri dan mengancam pertahanan nasional. Walaupun pemilihan umum di Indonesia masih dilakukan secara konvensional, tetapi teknologi informasi telah terimplementasi secara parsial pada beberapa sistem.

Berdasarkan Undang-undang Dasar 1945 Pasal 22E ayat 1 yang menyatakan bahwa "Pemilihan Umum dilaksanakan secara langsung, umum, bebas, rahasia, jujur dan adil setiap lima tahun sekali'. Hal-hal tersebut menjadi asas pelaksanaan pemilihan umum yang selama ini diikuti oleh pemerintah Indonesia. Komisi Pemilihan Umum sebagai badan penyelenggara pemilihan umum di Indonesia seharusnya dapat menjamin pelaksanaan pemilu sesuai asas-asas tersebut bagi masyarakat Indonesia. Pada kenyataannya bahwa pelaksanaan pemilu sejak beberapa tahun terakhir mengalami disrupsi. Terjadinya berbagai macam gangguan pada pelaksanaan pemilu yang pernah dialami menjadi bukti empiris bagaimana pemilu tidak lagi sesuai dengan asas-asas yang ada. Gangguan-gangguan tersebut merupakan implikasi dari era teknologi digital yang membuka spektrum

[8] Michael Smith. *Research Handbook on International Law and Cyberspace.* (Cheltenham UK: Edward Elgar Publishing Limited, 2015). hlm 2

ancaman yang lebih masif pada saat pemilu seperti berbagai ancaman yang dimulai dari misinformasi untuk mempengaruhi publik hingga serangan siber yang sering dialami oleh situs-situs miliki KPU pusat dan daerah.

Komisi Pemilihan Umum (KPU) sebagai penyelenggara pemilihan umum di Indonesia seharusnya dapat belajar dari pengalaman beberapa negara dalam pengamanan pemilu. Dengan perkembangan teknologi yang pesat serta penetrasinya dalam pemilihan umum, maka membuka peluang bagi ancaman yang lebih luas dalam ranah siber. Intensitas, frekuensi dan tipe serangan yang pernah terjadi pada pemilu di beberapa negara, seharusnya dapat dipelajari oleh pihak KPU untuk dapat mengidentifikasi pola serangan siber. Sehingga, ketika suatu serangan terjadi maka dapat diketahui tujuan (*purpose*), target (target), konteks (*context), dan* skala (*scale*).

Serangan siber yang pernah dialami oleh KPU yang terus bereskalasi dalam frekuensi, dan publisitas dari tahun ke tahun menjadi tantangan tersendiri dalam membentuk keamanan siber. Dalam menghadapi spektrum ancaman siber yang luas dan dengan kemajuan teknologi pada saat ini, KPU sepantasnya memiliki infrastruktur yang menunjang kinerjanya. Tetapi pada kenyataannya hal tersebut masih menjadi permasalahan yang harus dihadapi oleh KPU pada pelaksanaan pemilihan umum 2019 mendatang. Sehingga untuk mengatasi kekurangan tersebut, KPU membangun kerjasama dengan instansi-instansi lainnya.

Dalam pelaksanaan pemilu selama ini, KPU telah bekerjasama dengan pihak akademisi seperti Universitas Indonesia dan Institut Teknologi Bandung dalam pengembangan sistem informasi (SI) dan teknologi informasi (IT). Sedangkan sepanjang tahun 2017 hingga 2018, KPU berencana akan berkolaborasi dengan institusi-insitusi lain yang *trustworthy* dan *eligible* serta memiliki *capacity* dan *capability* dalam pengamanan informasi. Institusi-institusi seperti Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika (Kominfo), Badan Intelijen Negara (BIN), Kementerian Koordinator Politik, Hukum dan Keamanan serta *Cybercrime* POLRI akan turut berkontribusi dalam melakukan deteksi, proteksi serta prevensi terhadap ancaman dan serangan siber yang dapat terjadi pada Pemilu 2019.

Global Risks Landscape Report melalui surveinya pada tahun 2017 dan 2018 menempatkan serangan siber

(*cyberattacks*) dengan prioritas tertinggi dibandingkan dengan *interstate conflict* ataupun serangan teroris. Serangan siber sendiri memiliki berbagai bentuk seperti *Cyber War, Cyber Terrorism, Cyber Espionage* dan *Cyber Crime.* Ancaman-ancaman tersebut merupakan salah satu bentuk ancaman non-tradisional dan menjadi suatu isu yang tersekuritisasi karena mengancam eksistensi dan keamanan negara sebagai referen tertinggi yang mencakup keamanan militer, lingkungan, ekonomi, sosial dan politik. Dalam menghadapi ancaman-ancaman tersebut maka perlu dibangun suatu kemampuan pertahanan nirmiliter di dunia maya (*Cyberspace*) yang disebut dengan *Cybersecurity*. Keamanan siber (*Cybersecurity*) sendiri merupakan aktivitas untuk melakukan pengamanan terhadap sumber daya telematika demi mencegah terjadinya tindakan *Cybercrime.*

Berdasarkan *Conceptual Framework Global Cybersecurity Index* oleh *International Telecommunication Union (ITU),* Indonesia berada pada peringkat ke-70 dengan *score* 0.424 yang mengindikasikan bahwa Indonesia masih memiliki kelemahan dalam implementasi pilar keamanan siber. Dalam penelitiannya *Global Cybersecurity Index* menekankan tingkat keamanan siber pada lima pilar yaitu *legal, technical, organizational, capacity building* dan *cooperation.*

Pilar legal diukur berdasarkan keberadaan lembaga hukum dan kerangka kerja yang berhubungan dengan *cybersecurity* dan *cybercrime.* Pilar teknis diukur berdasarkan keberadaan lembaga teknis dan kerangka kerja yang berhubungan dengan keamanan siber. Pilar organisasi diukur berdasarkan keberadaan lembaga organisasi kebijakan dan strategi untuk pengembangan keamanan siber di tingkat nasional. Pilar Peningkatan Kapasitas yang diukur berdasarkan keberadaan penelitian dan pengembangan, pendidikan dan program pelatihan; profesional bersertifikat dan lembaga sektor publik yang mendukung kapasitas bangunan. Dan pilar kerjasama diukur berdasarkan keberadaan kemitraan, kerangka kerja koperasi dan jaringan berbagi informasi.[9]

Berdasarkan *Scorecard* di wilayah Asia dan Pasifik menurut Global security index 2017, menunjukkan komitmen dalam keamanan siber bahwa Indonesia masih memperoleh nilai rendah pada pilar *organizational* dan *cooperation* yang

[9] *Ibid* hlm 4

berarti masih lemahnya pemerintah dalam penerapan strategi yang terorganisir, koordinasi antar institusi serta kompilasi indikator dalam *tracking* kejahatan siber (*cybercrime*).

Perwujudan keamanan siber tidak dapat dilakukan secara sendiri, tetapi dibutuhkan kerjasama dengan instansi-instansi lainnya. Indonesia telah memasuki era keamanan siber 2.0 yang mengadopsi model kolaborasi diantara lembaga pemerintah, industri teknologi informasi dan perguruan tinggi yang cenderung menentukan arah perkembangan teknologi siber kedepan.

Dibawah ini merupakan peta ancaman yang terjadi pada pemilu baik sebelum pemilu dilaksanakan, sepanjangan pelaksanaan pemilu hingga ketika pemilu telah terlaksana.

Tabel 1. Peta Ancaman Pemilu

Jenis Ancaman	
Sebelum pemilihan	Ancaman sosiokultural berupa misinformasi atau *disinformation campaign*, hoax dll untuk mempengaruhi dan menggiring opini publik
Sepanjang pemilihan	Peretasan terhadap sistem (server, transmisi) untuk mempengaruhi berjalannya proses pemilihan
Setelah pemilihan	Peretasan terhadap sistem untuk memanipulasi hasil perhitungan suara

Sumber: Diolah oleh Peneliti, 2018

Dengan mengetahui indikator-indikator tersebut maka menjadi hal yang penting bagi publik untuk mengetahui bagaimana cara kerja sistem pemilihan umum pemerintah dan strategi tepat apa yang dapat diterapkan.

Berdasarkan permasalahan diatas, peneliti tertarik meneliti mengenai strategi Keamanan siber KPU Pusat dalam menghadapi Pemilihan Umum 2019 dalam membendung kemungkinan ancaman siber sebagai kajian dari peperangan asimetris dengan judul Strategi Keamanan Siber Komisi Pemilihan Umum (KPU) Pusat Dalam Menghadapi Pemilihan Umum 2019. Fokus penelitian ini adalah tentang bagaimana strategi keamanan siber yang akan diimplementasikan pada Pemilu, sinergitas antara KPU Pusat dengan institusi-institusi lainnya terkait aspek keamanan siber serta faktor-faktor penghambat yang dihadapi dalam mewujudkan keamanan siber tersebut pada Pelaksanaan Pemilu 2019.

Metode Penelitian

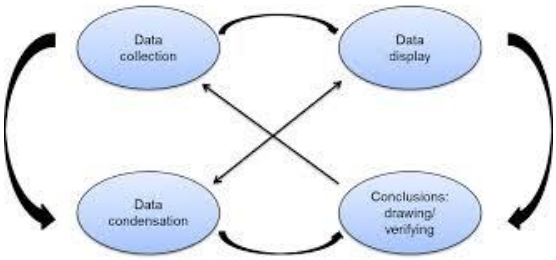
Penelitian tentang strategi keamanan siber Komisi Pemilihan Umum (KPU) Pusat dalam menghadapi Pemilu 2019 dilakukan dengan menggunakan metode penelitian kualitatif dengan pendekatan fenomenologi yang merupakan

pendekatan kualitatif dimana peneliti mengidentifikasi esensi dari pengalaman-pengalaman manusia mengenai sebuah fenomena yang sebagaimana digambarkan oleh partisipan. Pengalaman manusia dalam penelitian ini adalah pengalaman dari pihak-pihak yang terlibat langsung dari fenomena yang dikaji sebagai narasumber. Melalui metode kualitatif fenomenologi ini penulis akan mengkaji, mempelajari dan menganalisis secara komprehensif terkait strategi keamanan siber yang diimplementasikan Komisi Pemilihan Umum Pusat terutama pada aspek organisasional yang dianggap dapat membendung ancaman siber pada pemilu 2019.

Sumber data utama dalam penelitian kualitatif ini sendiri adalah berbagai informan yang menjadi subyek penelitian sehingga diperoleh beberapa data primer. Data primer diperoleh dari sumbernya secara langsung, diamati dan dicatat secara langsung, seperti wawancara, observasi, dan dokumentasi dengan pihak yang terkait atau informan yang mengetahui secara jelas dan rinci mengenai masalah yang sedang diteliti. Sedangkan data sekunder diperoleh dari data yang telah ada sebelumnya serta memiliki keterkaitan atau relevan dengan yang diteliti yaitu meliputi literatur-literatur yang ada, dokumen penting dan mendukung penelitian seperti dokumentasi.

Dalam pemilihan subyek penelitian, peneliti menggunakan teknik *Purposive sampling* dimana artinya adalah teknik pengambilan sampel sumber data, yang pada awalnya pengambilan data biasa menjadi difokuskan dan mendalam. Para informan telah ditentukan terlebih dahulu oleh peneliti. Informan dalam penelitian ini merupakan pihak-pihak yang memiliki kaitan erat dan terlibat langsung dalam permasalahan yang terjadi.

Teknik analisa data dilakukan dengan menggunakan teknik dari Miles dan Huberman dengan langkah-langkah yang dijabarkan pada gambar berikut:



Gambar 1. Analisa Data Kualitatif *Miles & Huberman*
Sumber: Miles & Huberman, *Qualitative Data Analysis, 2014*

Gambar di atas menunjukkan bahwa proses analisis data dilakukan secara bersamaan mulai dari pengumpulan data, kondensasi data, display data yang dilakukan secara berkesinambungan selama proses penelitian berlangsung. Langkah terakhir dalam proses analisis

data yang dilakukan adalah penarikan kesimpulan/ verifikasi data.

Pembahasan

Tujuan dari pembahasan adalah untuk mendapatkan hasil analisa serta gambaran yang jelas dan konkrit tentang hal-hal yang berhubungan dengan permasalahan yang diteliti. Hal ini dilakukan karena di dalam penelitian yang menggunakan pendekatan kualitatif akan membutuhkan lebih banyak penjelasan atau pembahasan serta penguraian secara sistematis, faktual dan akurat mengenai fakta-fakta dan karakteristik yang berbeda di lapangan. Oleh karena itu, peneliti berusaha untuk bersikap obyektif terkait permasalahan yang didapatkan dan memberikan pemahaman serta penjelasan kepada pembaca mengenai kejadian faktual dan interpretasi analisis hasil yang didapatkan di lapangan tanpa adanya unsur subyektifitas dari peneliti.

Strategi Keamanan Siber Komisi Pemilihan Umum (KPU) Pusat dalam Menghadapi Pemilu 2019

Guna mencapai tujuan yang telah direncanakan oleh KPU Pusat, maka dibutuhkan suatu strategi yang tepat. secara etimologis, strategi dalam manajemen organisasi dijabarkan sebagai kiat, cara dan taktik yang dipersiapkan secara sistematik dalam melakukan fungsi-fungsi manajemen yang terarah pada tujuan organisasi.

Guna menganalisa strategi keamanan siber yang diimplementasikan oleh KPU Pusat, Peneliti menggunakan pendekatan teori yang disampaikan oleh Carl Von Clausewitz dan dikembangkan oleh Kolonel Arthur F. Lykke Jr dimana dalam sebuah strategi dielaborasikan menjadi 3 substansi fundamental yaitu:[10]

a. *Ends* yang diinterpretasikan sebagai tujuan yang hendak dicapai dari sebuah strategi yang telah direncakanan.
b. *Means* diterjemahkan sebagai seluruh sumber daya atau instrumen yang dapat digunakan guna mendukung pencapaian tujuan dan
c. *Ways* merupakan cara yang ditempuh atau digunakan guna mencapai tujuan.

Ketiga substansi fundamental tersebut dibentuk kedalam formula:

"*Strategy = Ends + Ways + Means*"

Selain itu analisa terhadap strategi keamanan siber, juga didukung dari

[10] Baker N. & Stephens A., *Making Sense of War: Strategy for the 21st Century* (Cambridge: Cambridge University Press, 2006), hlm. 68

perpektif konsep manajemen stratejik yang dikemukakan oleh Agustini[11], yang menyatakan bahwa diperlukan analisa pada manajemen yang terdiri atas beberapa unsur yang berpengaruh terhadap pelaksanaan strategi yang dijabarkan sebagai berikut:

a. *Man Power* (Sumber Daya Manusia)
   Merupakan unsur fundamental dan krusial dengan alasan bahwa manusia berperan sebagai perancang dan penetap tujuan serta sekaligus berperan sebagai pelaksana dalam mencapai tujuan yang telah ditetapkan.
b. *Material* (Materi)
   Dalam mencapai tujuan dibutuhkan sarana dan prasaran yang berperan sebagai alat (*Means*) dalam mencapai tujuan.
c. *Machine* (Teknologi)
   Dengan hampir terkonvergensinya seluruh aspek kehidupan manusia dengan teknologi, maka menjadi salah satu faktor penentu dalam mencapai tujuan.
d. *Method* (Metode)
   Merupakan cara atau metode yang akan diimplementasikan guna mencapai tujuan.
e. *Money* (Uang)
   Faktor anggaran berkontribusi dalam mendukung proses pelaksanaan strategi.
f. *Market* (Pasar)

Dengan adanya manajemen stratejik tersebut diharapkan dapat mencapai tujuan yang diinginkan oleh KPU mengingat Pemilihan umum 2019 telah mengalami pergeseran dari pilkada dan pemilu 1.0 menuju pilkada dan pemilu 2.0. Pilkada dan Pemilu mengalami *upgrade* ditandai dengan semakin intensifnya peran sosial media sebagai medium opini publik. Kehadiran sosial media telah metransformasi medan politik dimana kejayaan diperoleh oleh tokoh dan partai yang memaksimalkan sosial media. Sehingga membuat spektrum ancaman lebih luas dimulai dari sosiokultural (*psychological warfare*) hingga peretasan. Potensi timbulnya beragam jenis ancaman tersebut dituangkan dalam timeline kerawanan dan peta ancaman siber. Dengan menganalisa *behavior* dan *pattern* serangan dan besarnya potensi ancaman yang dapat muncul pada titik-titik rawan, diharapkan dapat menjadi panduan dalam peningkatan keamanan siber pada pelaksanaan Pemilu kedepannya.

[11] Agustini, *Pengelolaan dan Unsur-unsur Manajemen.* (Jakarta: Citra Pustaka, 2013). Hlm. 61

Adapun *Ends* yang merupakan tujuan yang ingin dicapai oleh KPU sebagaimana termaktub pada Pasal 10 Undang-Undang Nomor 3 Tahun 1999 tentang Pemilihan Umum dan Pasal 2 Keputusan Presiden Nomor 16 Tahun 1999 tentang Pembentukan Komisi Pemilihan Umum dan Penetapan Organisasi dan Tata Kerja Sekretariat Umum Komisi Pemilihan Umum yang menyebutkan bahwa tugas kewenangan KPU adalah merencanakan dan mempersiapkan Pemilihan Umum. Tentunya perencanaan dan persiapan Pemilihan umum dilaksanakan secara komprehensif yang meliputi aspek fisik dan juga aspek virtual. Sehingga terwujud Pemilu yang LUBER dan JURDIL.

Dalam mencapai tujuannya (*Ends*), KPU pusat mengerahkan seluruh sumber daya (*resources*) dalam mengamankan Pemilu yang akan digelar dengan membangun kekuatan solid melalui kesiapan infrastruktur teknologi baik perangkat keras (*hardware),* perangkat lunak (*software*) ataupun pekerja (*Brainware)* yang dikonsolidasikan dari *stakeholders* yang terlibat. Adapun pengamanan dilakukan pada 4 (empat dimensi) yang diimplentasikan pada setiap organisasi termasuk KPU diantaranya aspek teknis terkait keamanan fisik, logis, lingkungan dan manajemen operasional, aspek manusia meliputi kesadaran, edukasi dan pengawasan, aspek legal terkait prosedur dan aturan atau legalitas, serta organisasional menyangkut misi, struktur, tanggung jawab dan manajemen stratejik.

Peraturan Menteri Pertahanan tentang Pedoman Pertahanan Siber menyebutkan salah satu agenda kebijakan keamanan siber adalah *organizational structure* (struktur organisasi) yang mengkaji terkait keberadaan kemitraan, kerangka kerjasama dan jaringan berbagi informasi dalam mewujudkan keamanan siber. Indonesia memasuki era keamanan siber 2.0 dimana keamanan siber dibentuk dengan mengadopsi model kolaborasi diantara lembaga pemerintah, industri teknologi informasi dan perguruan tinggi yang cenderung menentukan arah perkembangan teknologi siber kedepan. Berdasarkan kenyataan tersebut maka KPU mengadopsi strategi *collaborative approach* dengan konsep *Triple Helix* sebagai cara (*Ways*) yang meliputi komunikasi dan koordinasi dengan *stakeholders* dari pemerintah K/L, swasta dan akademisi. Kerjasama tersebut dilakukan guna membangun sistem penangkalan, penindakan dan pemulihan terhadap serangan siber yang dilakukan bersama *Stakeholders* dengan bidang

masing-masing. Dengan perancangan dan pengembangan aplikasi KPU bersama Akademisi, pembuatan dan penetapan aturan kampanye bersama Bawaslu, kegiatan pengamanan infrastruktur IT Pemilu yang dilakukan bersama Kemkominfo dan BSSN, kolaborasi pembuatan kebijakan terkait keamanan siber dengan K/L lain serta *collaboration action in Cyber threat intelligence* yang dilakukan oleh KPU dan K/L yang bersangkutan.

Sinergitas antara Komisi Pemilihan Umum (KPU) Pusat dengan *Stakeholders (Triple Helix)*

Sebagaimana manajemen dan teknologi tidak memungkinkan untuk menghindari insiden sepenuhnya dan tidak terdapatnya konsep "*zero risk*", maka masalah tanggung jawab menjadi sentral yang berhubungan dengan keamanan informasi. Sehingga untuk mewujudkan keamanan siber perlu ditekankan tentang perlunya koordinasi antar lembaga. Keamanan siber tidak dapat diwujudkan seorang diri, tetapi dibutuhkan kerjasama dengan instansi-instansi lainnya.

Surowiecki mengungkapkan bawah sinergitas merupakan suatu kolaborasi yang terbentuk antara beragam kelompok yang memiliki perspektif berbeda melalui kerjasama dengan tujuan meningkatkan efektifitas melalui kolaborasi pengetahuan, persepsi dan perspektif bersama. Dengan demikian untuk mengetahui tingkat sinergitas yang dilakukan oleh KPU Pusat dengan *stakeholders* dalam mencapai *Ends.*[12] Teori O. Gupta & G. Ross menyatakan bahwa terbangunnya sinergitas melalui dua cara yaitu komunikasi dan koordinasi.[13]

a. Komunikasi

Komunikasi dapat diartikan sebagai sebuah proses pertukaran informasi diantara individu-individu melalui suatu sistem simbolik, tanda-tanda ataupun sikap yang sama. Sebagai pihak yang bertanggung jawab langsung terhadap pelaksanaan Pemilu, maka KPU dalam upaya membangun keamanan siber berusaha untuk membangun komunikasi yang aktif dengan para

[12] Surowiecki, James. *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations*. (USA: Doubleday; Anchor. 2004).

[13] Gupta, O. & Roos, G. *Mergers and acquisitions through an intellectual capital perspective. Journal of Intellectual Capital*, 2(3). 2001. hlm. 297-309. & Krumm, J.M.M., Dewulf, G. & De Jonge, H. *Managing key resources and capabilities: pinpointing the added value of corporate real estate management. Facilities*, 16(12/13). 1998. hlm. 372-379

stakeholder lainnya. Model komunikasi dilakukan melalui *sharing information* dimulai dari bentuk konsultasi, diskusi hingga *Forum Groups Discussion (FGD)* yang melibatkan seluruh pemangku kepentingan yang kemudian dtindaklanjuti sebagai bentuk koordinasi dengan para *Stakeholders.*

b. Koordinasi

Komunikasi tidak dapat berdiri sendiri tanpa adanya koordinasi yang ditandai dengan 9 (sembilan) syarat dalam mewujudkan koordinasi yang efektif.[14] Kesembilan syarat tersebut sepenuhnya telah dipenuhi oleh KPU dalam rangka mewujudkan koordinasi yang efektif diantaranya melakukan hubungan pribadi langsung dengan para stakeholders yang terlibat, melakukan perencanaan dan pembuatan kebijakan pada awal kerjasama, mempertahankan koordinasi secara berkesinambungan pada seluruh aspek perencanaan dan dilakukan secara dinamis dengan tujuan yang telah ditetapkan, implementasi struktur organisasi yang sederhana, pembagian peran dan tanggung jawab yang jelas antar stakeholders yang didukung dengan komunikasi yang aktif dan efektif serta kepemimpinan yang supervisi.

Bentuk koordinasi yang terjalin antara KPU dan institusi-institusi lainnya yaitu dimulai dari pengembangan dan pengetesan aplikasi Pemilu dengan pihak Akademisi dan BPPT, identifikasi, pelaporan dan tindak lanjut atas pelaporan tersebut yang dilakukan oleh KPU, Bawaslu, Kominfo, Menkopolhukam dan *Cybercrime* POLRI. Selain itu, pengamanan dari sisi infrastruktur dilakukan bersama sama dengan BSSN, ID-SIRTII, BIN dan APJII.

Mengkaji dari 2 (dua) cara terbangunnya suatu sinergitas yang baik melalui komunikasi dan koordinasi, maka berdasarkan hasil temuan dan teori yang digunakan maka dapat dikatakan bahwa Komisi Pemilihan Umum (KPU) Pusat telah membangun sinergitas dengan para *stakeholders* dengan baik, hanya saja sinergitas tersebut belum terkonvergensi sepenuhnya dan belum mengikat dikarenakan belum adanya payung hukum yang melindungi serta mengatur peran dan tanggung jawab dari para *stakeholders*.

[14] Moekijat. *Koordinasi (Suatu Tinjauan Teoritis).* (Bandung: Mandar Maju, 1994). Hlm. 23

Faktor-faktor penghambat yang dihadapi oleh Komisi Pemilihan Umum (KPU) Pusat dalam implementasi keamanan siber

Pada sub-bab ini peneliti mengelaborasikan hasil penelitian terhadap rumusan masalah salah satunya mengenai faktor-faktor penghambat yang dihadapi oleh Komisi Pemilihan Umum (KPU) Pusat dalam mewujudkan keamanan siber pada pelaksanaan Pemilu 2019 yang dikaitkan dengan teori hambatan. Adapun hambatan-hambatan tersebut terdiri atas *budgeting, Human Power* dan *legal* yang akan dijelaskan sebagai berikut:

a. Budgeting/ Money

Faktor penghambat yang pertama dalam mewujudkan keamanan siber selama ini adalah adalah masalah anggaran yang dimiliki oleh KPU terutama pada Biro Perencanaan dan Data. Terjadinya ketidaksesuaian antara anggaran yang telah ditetapkan pada awal program dengan kebutuhan di lapangan pada saat pelaksanaan menjadi kendala dalam menghadapi ancaman keamanan siber terutama pada aspek infrastruktur dan sumber daya manusia.

Seiring dengan perkembangan teknologi yang eksponensial, maka jenis dan serangan siber juga mengalami peningkatan dan semakin *sophisticated*. Peretas menjadi lebih terampil dalam menemukan lubang dan kerentanan pada sistem keamanan yang menjadi ancaman keamanan siber. Sehingga dibutuhkan kesiapan dari segi infrastruktur teknologi dan juga peningkatan kemampuan dari sumber daya manusia. Dalam peningkatan kemampuan teknologi maka dibutuhkan anggaran yang tidak sedikit, apalagi dengan trend teknologi kini yang telah mengalami transformasi terus menerus, maka dibutuhkan perhatian pada anggaran infrastruktur.

b. Man Power

Faktor penghambat yang kedua dalam mewujudkan keamanan siber pada pemilu selama ini adalah *Man Power* (sumber daya manusia) yang dimiliki. KPU selama ini memiliki jumlah personil yang terbatas yang berjumlah 5 orang dengan rincian 3 orang organik KPU dan 2 orang Non-organik. Berdasarkan fungsi operasional manajemen sumber daya manusia yaitu pada pengadaan sumber daya manusia merupakan penentuan sumber daya yang dibutuhkan disesuaikan dengan tugas, perekrutan dan penempatan sumber daya.

Kemajuan teknologi yang pesat tidak diimbangi dengan sumber daya manusia yang professional yang memiliki *skill* dibidang IT, sehingga membentuk permasalahan *Cybersecurity Skill Crisis.* Hal ini tentunya membuat para professional IT terutama di bidang *cybersecurity* memiliki *demand* yang tinggi dengan upah yang tidak sedikit. Dengan *budget* terbatas yang dimiliki oleh KPU maka sulit untuk memperoleh pekerja professional di bidang IT terutama keamanan siber.

Disamping hal tersebut, diperlukan juga adanya edukasi dan sosialisasi dalam bentuk training atau pelatihan terhadap para pekerja dengan tujuan meningkatkan kesadaran akan keamanan informasi dan keamanan siber. Mengingat manusia adalah mata rantai yang lemah dalam rantai keamanan dank arena manusia adalah konsumen terakhir dari layanan dan infrastruktur TIK, solusi keamanan apapun juga harus mempertimbangkan kebutuhan sosial.[15]

Selanjutnya, kurangnya dokumentasi yang merupakan artefak yang seharusnya dipelihara sebagai dasar dan standar untuk pengembangan sistem keamanan dikarenakan pekerja yang terus berganti. Permasalahan ini kemudian memunculkan *lack of transfer knowledge* dari generasi sebelumnya ke generasi berikutnya untuk dapat mengetahui alasan dari setiap *design decision* yang dilakukan.

c. Legal

Selama ini KPU hanya terikat kerjasama dengan Bawaslu dan Kementerian Komunikasi dan Informatika yang juga melibatkan *social media platform* dan juga penyedia jasa internet (APJII) yang terikat dalam *Memorandum of Action* (MoA) yang dilakukan pada Pilkada 2018. Sedangkan menjelang kampanye Pemilihan umum Presiden, rancangan kerjasama tersebut masih dalam tahap perencanaan dan pengkajian untuk dapat disetujui oleh Rudiyantara selaku Menteri Komunikasi dan Informatika.

Sejalan dengan permasalahan tersebut, Badan Siber dan Sandi Negara (BSSN) sebagai lembaga yang bertanggung jawab dalam keamanan siber di Indonesia belum terikat dalam suatu kerjasama yang formal sebagai payung hukum yang mendasari

[15] Ghernaouti Solange. *Cyber Power*. (Switzerland: EPLF Press. 2013). Hlm. 331

kontribusinya dalam pengamanan siber pada Pemilu 2019. Tanpa adanya dasar legalitas maka BSSN tidak memiliki *legal standing,* sehingga tidak memiliki kewenangan dan tanggung jawab yang dapat dilaksanakan yang berada pada koridor hukum yang telah ditentukan. Legalitas tersebut berperan sebagai landasan kerja bagi BSSN untuk dapat berperan aktif dan memberikan kontribusi bagi KPU dalam menciptakan keamanan siber pada tiap-tiap tahapan Pemilu.

Dengan adanya payung hukum tersebut, BSSN dapat diikutsertakan dalam pengamanan siber. Baik itu dalam tahap desain, pengujian aplikasi hingga pengamanan infrastruktur pada saat pelaksanaan Pemilu. Pernyataan tersebut dipertegas oleh Informan C-3 yang mengatakan seharusnya terdapat suatu regulasi yang mengatur sejauh mana keterlibatan para *stakeholders*. Selain itu seharusnya juga terdapat regulasi di KPU sendiri yang mengatur kontrak para pekerja di bidang IT, sehingga tidak terjadi pergantian staf yang akan menyulitkan dokumentasi guna pengembangan sistem keamanan siber KPU.

Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan oleh Peneliti terkait strategi keamanan siber Komisi Pemilihan Umum (KPU) Pusat dalam menghadapi Pemilu 2019, maka dapat disimpulkan sebagai berikut:

1. Strategi keamanan siber yang diimplementasikan oleh Komisi Pemilihan Umum (KPU) Pusat pada pelaksanaan Pemilihan Umum 2019 adalah *Collaborative Approach* dengan konsep kerjasama *Triple Helix* yang melibatkan Pemerintah, Swasta dan Akademisi. Strategi tersebut meliputi deteksi, proteksi dan prevensi dari ancaman pada titik-titik kritis dan rawan pada saat sebelum, pelaksanaan dan pasca pemilu yang diharapkan dapat mendukung keberhasilan pelaksanaan Pemilu 2019 mendatang.
2. Sinergitas yang terbangun antara KPU dan *stakeholders* lainnya dapat dikatakan cukup baik dibandingkan dengan tahun-tahun sebelumnya. hal ini ditunjukkan dengan pemenuhan dari syarat sinergitas yaitu komunikasi dan koordinasi. Selain itu, terefleksi melalui deeskalasi peredaran konten-konten negatif di sosial media baik isu *hoax, hate-speech* ataupun *disinformation campaign.* Respon cepat dari *Social*

Media Platform dalam menanggapi permintaan KPU dan Bawaslu serta peran aktif POLRI sebagai *law enforcement* terhadap tindaklanjut laporan dari KPU dan Bawaslu. Selain itu, sinergitas yang terjalin tidak hanya sebatas diskusi ataupun FGD, tetapi juga telah mengalami peningkatan ke level teknis melalui *transfer of knowledge* dalam bentuk pelatihan, ataupun pelaporan yang dilakukan oleh pihak strategis lainnya. Sinergitas ini terkendala dalam legalitas dimana tidak terdapatnya dasar hukum sebagai dasar kerjasama.

3. Terdapat beberapa hambatan dalam implementasi keamanan siber pada Pemilu 2019 diantaranya:

   a. Budgeting/Money

   Dengan anggaran yang terbatas maka sulit bagi KPU untuk dapat mengimbangi cepatnya perkembangan teknologi yang diikuti oleh transformasi ancaman yang semakin luas dan beragam.

   b. Human Power

   Dengan jumlah personil terbatas dianggap masih kurang optimal untuk mendukung kinerja pihak IT. Permasalahan ini diperburuk dengan rendahnya tingkat *awareness* dari personel KPU yang terlibat langsung dalam Pemilu dikarenakan kurangnya edukasi dan sosialisasi mengenai keamanan informasi dan keamanan siber.

   c. Legal

   Belum terdapatnya payung hukum sebagai dasar legalitas untuk dapat bekerjasama dengan para *stakeholders* lainnya, terutama dari instansi Pemerintah seperti Badan Siber dan Sandi Negara yang memiliki tanggung jawab dalam keamanan siber di Indonesia. Hambatan ini memberikan keterbatasan bagi BSSN dan *stakeholders* lainnya untuk dapat ikut terjun secara langsung dalam pengamanan siber pada pelaksanaan Pemilu 2019.

Rekomendasi

Berdasarkan dari kesimpulan di atas, maka peneliti memberikan beberapa rekomendasi kepada pemangku kebijakan sebagai bahan masukan. Seperti:

1. Strategi keamanan siber yang diimplementasikan oleh Komisi Pemilihan Umum (KPU) Pusat pada pelaksanaan Pemilihan Umum 2019 adalah *Collaborative Approach* dengan konsep kerjasama *Triple Helix* yang melibatkan Pemerintah, Swasta dan

Akademisi. Strategi tersebut meliputi deteksi, proteksi dan prevensi dari ancaman pada titik-titik kritis dan rawan pada saat sebelum, pelaksanaan dan pasca pemilu yang diharapkan dapat mendukung keberhasilan pelaksanaan Pemilu 2019 mendatang.

2. Sinergitas yang terbangun antara KPU dan *stakeholders* lainnya dapat dikatakan cukup baik dibandingkan dengan tahun-tahun sebelumnya. hal ini ditunjukkan dengan pemenuhan dari syarat sinergitas yaitu komunikasi dan koordinasi. Selain itu, terefleksi melalui deeskalasi peredaran konten-konten negatif di sosial media baik isu *hoax, hate-speech* ataupun *disinformation campaign.* Respon cepat dari *Social Media Platform* dalam menanggapi permintaan KPU dan Bawaslu serta peran aktif POLRI sebagai *law enforcement* terhadap tindaklanjut laporan dari KPU dan Bawaslu. Selain itu, sinergitas yang terjalin tidak hanya sebatas diskusi ataupun FGD, tetapi juga telah mengalami peningkatan ke level teknis melalui *transfer of knowledge* dalam bentuk pelatihan, ataupun pelaporan yang dilakukan oleh pihak strategis lainnya. Sinergitas ini terkendala dalam legalitas dimana tidak terdapatnya dasar hukum sebagai dasar kerjasama.
3. Terdapat beberapa hambatan dalam implementasi keamanan siber pada Pemilu 2019 diantaranya:

   a. Budgeting/Money

   Permasalahan anggaran merupakan faktor pertama yang menghambat IT KPU dalam mengembangkan keamanan siber dari segi infrastruktur dan sumber daya manusia. Dengan anggaran yang terbatas maka sulit bagi KPU untuk dapat mengimbangi cepatnya perkembangan teknologi yang diikuti oleh transformasi ancaman yang semakin luas dan beragam.

   b. Human Power

   Aspek sumber daya manusia menjadi faktor penghambat kedua bagi IT KPU dalam mewujudkan keamanan siber. Dengan jumlah personil terbatas dianggap masih kurang optimal untuk mendukung kinerja pihak IT. Permasalahan ini diperburuk dengan rendahnya tingkat *awareness* dari personel KPU yang terlibat langsung dalam Pemilu dikarenakan kurangnya edukasi dan sosialisasi mengenai keamanan informasi dan keamanan siber.

c. Legal

Belum terdapatnya payung hukum sebagai dasar legalitas untuk dapat bekerjasama dengan para *stakeholders* lainnya, terutama dari instansi Pemerintah seperti Badan Siber dan Sandi Negara yang memiliki tanggung jawab dalam keamanan siber di Indonesia. Hambatan ini memberikan keterbatasan bagi BSSN dan *stakeholders* lainnya untuk dapat ikut terjun secara langsung dalam pengamanan siber pada pelaksanaan Pemilu 2019.

Daftar Pustaka

Agustini. 2013. *Pengelolaan dan Unsur-unsur Manajemen.* Jakarta: Citra Pustaka.

Albrow, Martin and Elizabeth King (eds). 1990. *Globalization, Knowledge, and Society.* London:Sage Publication

Baker N. & Stephens A. 2006. *Making Sense of War: Strategy for the 21st Century* Cambridge: Cambridge University Press

Ghernaouti, Solange. 2013. *Cyber Power*. Switzerland: EPLF Press

James A. Green. 2015. *Cyber Warfare A Multidiciplinary Analysis.* Lanchester University: Routledge Studies in Conflict, Security and Technology.

Krisna. 2005. *Pengaruh Globalisasi Terhadap Pluralisme Kebudayaan Manusia di Negara Berkembang.* Public Journal

Michael Smith. 2015. *Research Handbook on International Law and Cyberspace.* (Cheltenham UK: Edward Elgar Publishing Limited)

Moekijat. 1994. *Koordinasi (Suatu Tinjauan Teoritis).* Bandung: Mandar Maju.

Scholte, J.A. 2000. *Globalization: A Critical Introduction.* London: Palgrave.

Surowiecki, James. 2004. *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations*. USA: Doubleday; Anchor.

Jurnal

Gupta, O. & Roos, G. 1998. *Mergers and acquisitions through an intellectual capital perspective. Journal of Intellectual Capital*, 2(3). 2001. hlm. 297-309. & Krumm, J.M.M., Dewulf, G. & De Jonge, H. *Managing key resources and capabilities: pinpointing the added value of corporate real estate management. Facilities*, 16(12/13).