Jurnal Humaniora Revolusioner

JHR, 9 (9), September 2025
ISSN : 24475540

KONTRIBUSI BADAN PENGEMBANGAN SUMBER DAYA MANUSIA PROVINSI JAWA TIMUR DALAM MENANGANI ANCAMAN KEJAHATAN SIBER TERHADAP ASN DI ERA GLOBALISASI BIROKRASI DIGITAL

Akmal Farrel Maulana[1], Abid Rohman[2]
Email: akmalmal3004@gmail.com[1]

Universitas Islam Negeri Sunan Ampel Surabaya

Abstrak: Transformasi digital dalam birokrasi pemerintahan telah membawa perubahan signifikan terhadap pola kerja Aparatur Sipil Negara (ASN). Tranformasi ini juga telah menghadirkan ancaman baru berupa kejahatan siber. Riset ini bertujuan untuk menganalisis kontribusi Badan Pengembangan Sumber Daya Manusia (BPSDM) Provinsi Jawa Timur sebagai aktor lokal dalam menghadapi ancaman kejahatan siber terhadap ASN di tengah dinamika globalisasi. Riset ini akan menggunakan pendekatan kualitatif deskriptif dan kerangka global governance dari Weiss dan Wilkinson. Dalam konteks ini, BPSDM berkontribusi melalui program seperti ASN Belajar dan Leadership Update Forum dalam merespon pentingnya untuk mengangani ancaman kejahatan siber di era birokrasi digital. Upaya ini menunjukan bahwa BPSDM telah memainkan peran penting dalam membangun kesadaran digital ASN dengan meninternalisasi norma-norma global seperti zero trust, cognitive triangle, dan resilience mindset kedalam sistem birokrasi lokal. Namun, tantangan struktural dan psikososial seperti belum terintegrasinya pelatihan dengan kebijakan teknis serta rendahnya kesadaran digital ASN masih menjadi hambatan bagi BPSDM Jawa Timur. Meski demikian, langkah-langkah yang dilakukan BPSDM telah mencerminkan aktor otonomi lokal dalam menanggapi tekanan global sebagai bentuk dari developmental human security dalam ruang birokrasi digital. Dengan demikian, kontribusi BPSDM dapat dipahami sebagai bagian dari tata kelola global yang bersifat multilayered dan kolaboratif. yang berperan aktif dalam membentuk dan meningkatkan sistem birokrasi digital yang lebih efesien dan inklusif.
Kata Kunci: Bpsdm Jawa Timur, Kejahatan Siber, Aparatur Sipil Negara, Global Governance, Human Security.

PENDAHULUAN

Perkembangan teknologi saat ini telah membawa transformasi terhadap sistem birokrasi pemerintahan. Aparatur Sipil Negara saat ini di tuntut untuk inovatif dan revolusioner terutama dalam memanfaatkan kemajuan teknologi agar dapat meningkatkan kinerja mereka dalam praktik pemerintahan. Badan Pengembangan Sumber Daya manusia Provinsi Jawa Timur sebagai lembaga pemerintahan daerah yang bertanggung jawab untuk mengembangkan kualitas sumber daya manusia memiliki peran penting dalam mecentak para Aparatur Sipil Negara yang berkualitas dan berdaya saing global. Maka dari itu, ditengah dinamika reformasi birokrasi yang terus berkembang, meskipun kemajuan teknologi digital saat ini telah memudahkan para ASN dalam praktik kerja birokrasi pemerintahan. Kemajuan teknologi digital ini juga menghadirkan tantangan serius yang berupa tindak kejahatan melalui teknologi digital yang semakin sering menyasar individu sebagai target utama. Hal ini di karenakan, perkembangan teknologi digital saat ini telah menciptakan transformasi besar dalam berbagai sektor kehidupan, khususnya dalam praktik kerja di instansi pemerintahan. Pemanfaatan teknologi digital seperti media sosial, aplikasi komunikasi daring, hingga platform transaksi digital saat ini menjadi bagian yang tidak dapat dipisahkan dari aktivitas pekerjaan para aparatur sipil negara. Minimnya pengetahuan dini tentang kejahatan siber dalam pemanfaatan teknologi secara tidak langsung telah membuka peluang bagi para oknum kejahatan siber untuk melancarkan aksinya. Kejahatan seperti hacking, phishing, online harassment telah sangat marak terjadi pada era saat ini.1

Berdasarkan hal tersebut, kejahatan seperti phising, hacking, dan lain sebagainya yang menimpa para ASN tidak hanya merugikan secara finansial. Kejahatan ini juga tidak hanya berdampak pada sisi teknis atau sistemik saja, tetapi juga menyentuh langsung aspek-aspek personal seperti rasa aman, kepercayaan diri, dan ketenangan mental seseorang ASN dalam beraktivitas di ruang digital.2 Dalam konteks birokrasi, serangan semacam ini dapat menurunkan efisiensi kerja, menghambat koordinasi, serta menciptakan rasa tidak percaya para ASN terhadap sistem teknologi yang digunakan. Kejahatan siber sendiri tidak lagi bersifat lokal, melainkan termasuk bentuk kejahatan lintas negara (transnasional) yang memerlukan respons strategis.

Dalam konteks ini, BPSDM Provinsi Jawa Timur sebagai lembaga yang bertanggung jawab atas pengembangan kapasitas ASN memiliki peran penting dalam menanggapi dan mengantisipasi kejahatan siber yang mengancam ASN sebagai pilar utama pemerintahan. Maka dari itu, penting untuk melihat bagaimana kotribusi BPSDM Jatim dalam menanggapi kasus kejahatan siber yang mengancam para ASN, serta apakah tantangan yang dihadapi oleh BPSDM dalam menanggapi kasus kejahatan siber ini.

Dalam upaya memahami posisi BPSDM dalam merespons ancaman kejahatan siber. Pendekatan konseptual yang mampu menjelaskan keterkaitan antara tanggung jawab lokal dan dinamika global sangat penting untuk digunakan untuk memahami lebih dalam fokus yang akan dikaji. Oleh karena itu, riset ini akan bertumpu pada kerangka Global Governance sebagaimana dijelaskan oleh Thomas G. Weiss dan Rorden Wilkinson. Mereka menegaskan bahwa global governance mencakup seluruh cara baik formal maupun informal di mana kehidupan global diatur oleh aktor-aktor lokal seperti lembaga daerah.3 Maka dari itu, kontribusi BPSDM terhadap perlindungan ASN dari kejahatan siber tidak bisa dipisahkan dari dinamika global di karenakan kejahatan siber adalah bagian dari realitas governance transnasional.

LANDASAN KONSEPTUAL

- Global Governance sebagai Kerangka Pemahaman

Konsep global governance merujuk pada serangkaian mekanisme, institusi, aktor, dan norma yang digunakan untuk mengatur hubungan global serta merespons tantangan transnasional di luar kendali satu negara atau institusi tunggal. Menurut Weiss dan Wilkinson, global governance mencakup seluruh cara baik formal maupun informal di mana dunia diatur termasuk oleh aktor negara, organisasi internasional, perusahaan swasta, LSM, hingga mekanisme pasar dan jaringan transnasional. Dalam konteks kejahatan siber, global governance menjadi pandangan yang sesuai dan penting untuk memahami bagaimana tantangan global seperti cybercrime tidak hanya ditanggapi oleh aktor global seperti PBB atau ITU saja melainkan aktor sub-nasional juga. Maka dari itu, BPSDM Jawa Timur sebagai aktor sub-nasional harus menjalankan peran penting dalam

menangani ancaman kejahatan siber terhadap ASN. Hal ini, sejalan dengan pandangan Weiss dan Wilkinson bahawa konsep global governance saat ini mencakup dimensi multilevel, yang dimana cakupannya mulai dari global hingga lokal serta mencakup interaksi antar aktor negara dan non- negara.4

METODE PENELITIAN

Penelitian ini disusun dengan menggunakan pendekatan kualitatif karena fokus yang diangkat menuntut pemahaman mendalam terhadap proses kelembagaan dalam mengkaji kontribusi BPSDM Jawa Timur terhadap perlindungan ASN dari ancaman kejahatan siber. Pendekatan kualitatif memungkinkan peneliti untuk menggali dinamika internal institusi, keadaan sosial, serta logika kebijakan yang diambil dalam menghadapi tantangan global yang kompleks. Maka dari itu, dengan menggunakan metode kualitatif deskriptif akan menggambarkan secara rinci bentuk-bentuk respons serta kebijakan BPSDM dan memahami temuan tersebut dalam kerangka global governance. Bertempat di BPSDM Provinsi Jawa Timur Surabaya, penelitian ini dilakukan secara langsung selama peneliti

melaksanakan kegiatan magang pada April hingga Juni 2025. Dalam proses pengumpulan data, peneliti menggunakan tiga teknik utama yakni pertama, melakukan wawancara mendalam kepada para ASN terutama mereka yang memiliki pengetahuan mengenai kasus-kasus kejahatan siber yang pernah menimpa ASN di BPSDM Jatim. Wawancara ini dilakukan secara terbuka namun terarah untuk menangkap narasi secara jujur. Kedua, observasi partisipatif digunakan sebagai teknik pelengkap. Peneliti secara aktif terlibat dalam kegiatan di BPSDM seperti menyaksikan bagaimana ASN menggunakan sistem digital, memperhatikan pola respons terhadap potensi risiko kejahatan siber baik yang di sadari maupun tidak di sadari oleh para ASN, dan mengikuti kegiatan sosialisasi yang diselenggarakan BPSDM. Observasi ini penting untuk menghindari ketergantungan penuh pada narasi verbal. Ketiga, menggunakan dokumen seperti jurnal, buku, ataupun riset penelitian yang relavan dengan isu yang diangkat. Hal ini dilakukan agar lebih memahami lebih dalam tentang isu yang diangkat. Dalam memastikan kredibilitas data peneliti menggunakan teknik triangulasi, yakni membandingkan antara wawancara, observasi, dan dokumen yang ada untuk melihat konsistensi dan menghindari

bias interpretatif. Dengan demikian, metode penelitian ini tidak hanya dimaksudkan untuk membuktikan asumsi awal. Hal ini menjadi sarana reflektif untuk melihat bagaimana sebuah institusi pemerintah daerah menavigasi perannya dalam lanskap ancaman global dalam konteks perlindungan ASN sebagai garda depan birokrasi terhadap ancaman kejahatan siber.

HASIL DAN PEMBAHASAN

Hasil

A. Bentuk Ancaman Kejahatan Siber terhadap ASN di BPSDM Jawa Timur

Era digitalisasi birokrasi pada saat ini telah membawa transformasi besar dalam pola kerja Aparatur Sipil Negara (ASN). Aparatur Sipil Negara sebagai pilar birokrasi pemerintahan dan garda terdepan pelayanan masyarakat sangat berperan penting dalam menjaga stabilitas jalannya sektor pemerintahan negara. Namun, dalam era transformasi birokrasi digital saat ini masih banyak para ASN yang masih minim pengetahuan tentang kejahatan siber. Hal ini dipengaruhi oleh minimnya sosialisi atau kepelatihan mengenai pengamanan atau deteksi dini terhadap ancaman kejahatan berbasis teknologi digital. Berdasarkan hal ini, celah-celah baru bagi bentuk kejahatan non-tradisional yang menyasar langsung pada individu seperti phishing dan hacking telah terbuka lebar.

Berdasarkan hasil wawancara dengan beberapa pihak terkait dan observasi yang dilakukan secara langsung dilapangan. Terdapat beberapa kasus yang ditemukan seperti seorang ASN berinisial IK yang telah menjadi korban penipuan online saat melakukan transaksi di marketplace Facebook. Berdasarkan peryataan korban “Saya baru sadar kalau telah tertipu waktu saya mencoba menghubungi pelaku tetapi pelaku sudah tidak bisa dihubungi,” ujar korban setelah baru menyadari dirinya telah tertipu. Kejadian tersebut telah membuat korban mengalami kerugian secara finansial, meskipun kerugian yang di derita korban tergolong kecil pada keyataanya dampak yang dirasakan tidak berhenti di situ. IK mengaku mengalami trauma secara psikologis, perasaan malu, hingga kehilangan kepercayaan diri dalam menggunakan media digital baik untuk kepentingan pribadi maupun pekerjaan. Lebih dari itu, peristiwa ini menciptakan perasaan khawatir yang berlebihan antara dirinya dan ruang digital yang seharusnya mendukung efisiensi kerjanya. Di sisi lain, teridentifikasi juga korban penipuan kejahatan siber yang hampir serupa yakni korban berinisial IT. Berdasarkan keterangan korban yang juga seorang ASN, IT mengalami

modus phishing yang lebih canggih. Korban mengungkapkan bahwa dirinya menerima file undangan dari nomor tidak dikenal melalui WhatsApp. Tanpa memverifikasi identitas pengirim terlebih dahulu, IT lantas membuka file tersebut yang mengarah ke situs web asing. Beberapa jam setelahnya, akun mobile banking IT mendapat sebuah notifikasi sebuah transaksi dan IT memastikan bahwa rekening yang dituju tidak dikenali oleh korban. IT merasa curiga bahwa akun mobile banking miliknya telah diretas, dikarenakan korban tidak

merasa melakukan transaksi sebesar Rp150.000 ke rekening tersebut. Berdasarkan hal tersebut, korban lantas pergi ke kantor bank untuk menanyakan perihal transaksi misterius yang terjadi. Pada awalnya IT yang sempat menganggapnya hanya gangguan biasa, korban kemudian merasa terkejut setelah pihak bank mengonfirmasi bahwa akunnya telah disusupi oleh pihak tidak bertanggung jawab.

Dari kedua kasus ini, terlihat bahwa pelaku memanfaatkan tiga elemen utama dalam upaya phishing atau penipuannya yakni rasa percaya, ketidaktahuan terhadap prosedur keamanan digital, dan pendekatan personal melalui platform digital umum seperti media sosial. Hal ini sejalan dengan temuan Octo Iskandar yang menyatakan bahwa phishing adalah bentuk rekayasa sosial modern yang menggabungkan elemen manipulatif dan celah psikologis korban, terutama saat teknologi digunakan tanpa pemahaman yang memadai.5 Secara keseluruhan, kasus-kasus ini membuktikan bahwa ancaman kejahatan siber terhadap ASN di BPSDM Jatim bersifat multidimensi. Kejahatan siber bukan hanya serangan terhadap data, tetapi serangan terhadap rasa aman individu yang akan berdampak sistemik pada kinerja kelembagaan. Dalam konteks ini, ruang digital bukan hanya infrastruktur kerja tetapi juga ruang hidup personal ASN. Ketika ruang ini dirusak oleh serangan seperti phishing, maka serangan tersebut telah menjadi tindakan pelanggaran terhadap martabat dan keamanan dasar manusia. Dengan demikian, kejahatan siber yang dialami oleh ASN BPSDM Jatim dapat dipahami sebagai bagian dari ancaman kontemporer yang menuntut respons kelembagaan yang serius. Berdasarkan peryataan tersebut, bisa di tegaskan bahwa bentuk kejahatan siber yang menimpa ASN bukanlah hal yang tidak penting. Kejahatan siber merupakan bagian dari tantangan structural yang nyata dalam birokrasi digital yang harus dikenali secara sistemik dan penting untuk segera ditangani.

B. Respons dan Kontribusi BPSDM terhadap Ancaman Kejahatan Siber

Menghadapi realitas kejahatan siber yang semakin canggih dan bersifat lintas batas. BPSDM Provinsi Jawa Timur mulai membangun kesadaran bahwa perlindungan terhadap ASN tidak hanya bisa dilakukan melalui pendekatan administrative, tetapi juga melalui strategi edukatif dan kolaboratif yang berorientasi pada penguatan kapasitas. Hal ini, menjadi titik balik yang penting dalam memahami kontribusi kelembagaan BPSDM yang meskipun bukan institusi teknis di bidang keamanan digital. BPSDM juga memegang peran strategis dalam memperkuat ketahanan individu ASN terhadap ancaman global.

Salah satu contoh nyata dari respons dan kontribusi tersebut terlihat dari di selenggarakannya webinar ASN Belajar Seri 11 (2023) yang secara tematik membahas Cyber Security. Dalam sesi ini, sebagai seorang narasumber Ardi Sutedja yang merupakan pendiri sekaligus ketua Indonesia Cyber Security Forum. Beliau menyampaikan bahwa peretas tidak lagi hanya menyerang perangkat keras, tetapi menargetkan pikiran dan emosi manusia. Berdasarkan permaparan tersebut, belia menyebut hal ini sebagai cognitive triangle yakni kombinasi manipulasi logika, emosi, dan psikologi sosial. Hal ini memperkuat argumen bahwa manusia adalah titik terlemah sekaligus titik masuk utama dalam ekosistem keamanan digital. Selain itu, beliau juga menekankan tentang pentingnya prinsip zero trust dalam kerangka pola pikir keamanan digital yang sudah lama dilupakan. Dimana pola pikir ini akan memberikan pandangan yang jelas bahwa ASN tidak hanya butuh teknologi, tetapi juga kesadaran kritis dalam menghadapi jebakan digital yang menyerang ruang-ruang kognitif mereka sebagai individu dan sebagai bagian dari sistem pemerintahan. Dengan menghadirkan tema ini dalam program ASN Belajar, BPSDM menunjukkan kontribusinya sebagai produsen kesadaran kelembagaan (institutional awareness). Meskipun upaya yang diambil oleh BPSDM ini belum berbentuk kebijakan teknis, ASN Belajar Seri 11 merupakan langkah penting dalam membangun kerangka mental bagi ASN untuk mengenali dan menghadapi serangan siber berbasis manipulasi psikologis. Langkah-langkah dan upaya yang dilakukan oleh BPSDM Jatim ini sejalan dengan pendekatan global governance seperti dijelaskan Weiss dan Wilkinson. Weiss dan Wilkinson menekankan bahwa aktor-aktor lokal juga memiliki kapasitas governance melalui proses normatif dan edukatif yang mempengaruhi pola

pikir dan perilaku para pegawai birokrasi.6 Berdasarkan peryataan tersebut, dapat di katakan bahwa BPSDM tidak semata-mata bertindak sebagai penyelenggara pelatihan saja tetapi juga sebagai aktor yang berperan dalam formasi norma global secara lokal.

Tidak hanya itu, BPSDM juga telah memperluas kontribusinya melalui penyelenggaraan Leadership Update Forum (LUF) Seri 2 tahun 2024 dengan tema Cyber Security Care. Forum ini dihadiri oleh para pejabat eselon serta seluruh kepala perangkat daerah yang ada di Jawa Timur. Dalam penyelenggaraan LUF ini BPSDM juga berkolaborasi dengan BSSN RI dan Dinas Kominfo Jawa Timur sebagai mitra strategis untuk menangani atau memberikan sosialisasi mengenai kejahatan siber. Dalam forum ini BPSDM secara strategis menyasar para pejabat eselon dan kepala perangkat daerah untuk memperluas cakupan kesadaran siber ke level pengambil kebijakan. Hal ini diperkuat dengan sambutan Kepala BPSDM Jatim yang menekankan bahwa kegiatan ini bertujuan untuk meningkatkan awareness dan mendorong tindakan preventif kelembagaan. Tidak hanya itu, kegiatan ini juga bertujuan untuk mendorong para ASN untuk melindungi data, jaringan, dan perangkat lunak dari kejahatan siber berbasis teknologi digital.

Berdasarkan hal tersebut, jika ditarik ke dalam lensa human security sebagaimana ditawarkan oleh Caroline Thomas. Kontribusi BPSDM ini dapat di lihat sebagai bentuk intervensi negara melalui lembaga daerah untuk memastikan hak-hak keamanan digital ASN sebagai bagian dari martabat dan otonomi personal. Thomas menegaskan bahwa keamanan manusia tidak bisa direduksi menjadi perlindungan fisik semata, melainkan juga mencakup jaminan partisipasi bermartabat dalam kehidupan sosial termasuk dalam ruang digital birokrasi.7 Maka dari itu, pelatihan keamanan digital yang dilakukan oleh BPSDM tidak hanya soal teknis tetapi juga merupakan bentuk penguatan terhadap kualitas ASN sebagai warga negara yang menggunakan teknologi digital. Dengan demikian, kontribusi BPSDM dalam menangani kejahatan siber terhadap ASN dapat dikategorikan sebagai respons edukatif-normatif yang mengarah pada penguatan kapasitas ASN melalui pendekatan kolaboratif dan multisektoral. Langkah ini menunjukkan bahwa BPSDM tidak hanya sekadar responsif terhadap ancaman global seperti kejahatan siber. BPSDM juga dapat di nyatakan telah berpartisipasi dalam membentuk global

governance dari bawah yang dimana keamanan ASN diakui sebagai bagian dari dimensi Human Security dalam ekosistem birokrasi digital modern.

Pembahasan

A. Kontribusi BPSDM sebagai Aktor Lokal dalam Menangani Isu Global: Cyber Crime

Fenomena kejahatan siber yang semakin kompleks telah menuntut kehadiran aktor lokal yang responsif terhadap dinamika global. Dalam konteks ini, Badan Pengembangan Sumber Daya Manusia (BPSDM) Jawa Timur memainkan peran penting sebagai institusi sub-nasional yang tidak hanya bersifat administratif tetapi juga edukatif dan normatif. Dalam hal ini, BPSDM telah berkontribusi secara langsung dalam membentuk kesadaran dan kapasitas ASN mengenai ancaman kejahatan siber. BPSDM Jatim telah membuktikkan bahwa aktor sub-nasional juga dapat aktif melalui serangkaian kegiatan yang mencerminkan praktik global governance berbasis multilayered dan multi-aktor. Praktik ini sekaligus menjadi refleksi atas transformasi tata kelola kontemporer yang bergerak dari model sentralistik menuju distribusi peran di antara aktor-aktor lintas level dan sektor.

Sebagai aktor lokal, BPSDM tidak sekadar menjalankan tugas nya sebagai lembaga peningkatan kualitas sumber daya manusia. BPSDM Jatim juga turut serta dalam membangun kesadaran institusional terhadap isu global seperti kejahatan siber. Inisiatif yang telah dilakukan BPSDM seperti menggelar ASN Belajar Seri 11 2023 dan Leadership Update Forum Seri 2 2024 yang dimana kedua program ini membahas tentang Cyber Security. Membuktikan bahwa BPSDM telah berkontribusi terhadap ancaman kejahatan siber yang mengancam para ASN di era birokrasi digital saat ini. Dalam upayanya ini, BPSDM menempatkan posisi sebagai fasilitator edukasi publik yang memediasi wacana lokal dengan diskursus global terkait keamanan digital. Keterlibatan tokoh para ahli seperti Ardi Sutedja

dari ICSF menandakan bahwa BPSDM secara aktif mengundang partisipasi dari epistemic community nasional. Hal ini, sesuai dengan pemahaman mengenai peran komunitas pengetahuan dalam membentuk agenda global governance. Kegiatan ini mencerminkan apa yang disebut oleh Weiss dan Wilkinson sebagai distributed authority, yakni pembagian otoritas dalam tata kelola global kepada aktor non-negara

dan subnasional.8 Dalam kerangka ini, BPSDM telah menunjukkan kapasitas institusional juga dapat menjadi aktor lokal dalam jaringan transnasional tentang pengarusutamaan norma keamanan digital.

B. Dinamika dan Tantangan BPSDM Jatim dalam Menangani Ancaman Kejahatan Siber

Berdasarkan pemaparan diatas, meskipun BPSDM telah berperan aktif dalam pencegahan ancaman kejahatan siber. BPSDM juga dihadapkan dengan berbagai tantangan dan dinamika yang harus dihadapi dalam upayanya menangani kasus kejahatan siber ini. Berdasarkan aspek struktural, hasil observasi menunjukkan bahwa belum ada integrasi antara pelatihan edukatif dan kebijakan institusional yang bersifat teknis. Dengan begitu, hasil pelatihan seringkali hanya berdampak terhadap peningkatan pengetahuan para ASN tanpa diikuti oleh perubahan sistem atau kebijakan organisasi yang bersifat preventif. Tidak hanya itu, jika dilihat dari sisi psikososial, rendahnya kesadaran kognitif para ASN terhadap ancaman siber menjadi titik lemah yang membuka peluang bagi para oknum kejahatan siber untuk memanipulasi keadaan seperti rekayasa sosial. Serangan melalui social engineering seperti mengeksploitasi kepercayaan dan memanfaatkan bias psikologis individu untuk melewati sistem keamanan.9 Merupakan teknik yang sekarang digunakan para hacker atau oknum kejahatan siber untuk melancarkan aksinya. Dalam konteks birokrasi, kerentanan ini dipicu oleh dominasi struktur birokrasi yang hierarkis sehingga membuat pegawai lebih rentan terhadap pola komunikasi manipulatif terutama ketika tidak dibekali oleh kewaspadaan digital. Hal ini telah menjadi tantangan yang sangat krusial dan penting untuk ditangani oleh BPSDM Jatim. Dikarenakan meskipun program yang di jalankan bisa dibilang telah berhasil meningkatkan pemahaman para ASN untuk melawan ancaman kejahatan siber. Masih terdapat celah yang harus di evaluasi lebih mendalam lagi supaya upaya pencegahan terhadap kejahatan siber lebih efektif.

C. Pengimplementasian Norma-Norma Global dalam Birokrasi Lokal

Lebih lanjut, meskipun masih terdapat celah yang harus di evaluasi lebih dalam lagi. Langkah-langkah edukatif yang dilakukan BPSDM terutama melalui narasi zero trust, cognitive

triangle, dan pentingnya membangun resilience mindset. Menunjukkan bahwa BPSDM telah meninternalisasi norma global dalam ruang birokrasi lokal. Dalam konsep global governance, proses ini disebut sebagai norm diffusion yakni ketika nilai-nilai universal seperti hak atas perlindungan data, privasi digital, dan etika online dikontekstualisasikan dalam realitas kebijakan domestik.10 Maka dari itu, prinsip sustainability in digital society menjadi relevan dalam konteks ini. Thomas Osburg menegaskan bahwa dalam konteks transformasi digital, literasi digital tidak bisa hanya berhenti pada pengetahuan tetapi harus melibatkan prinsip keberlanjutan, kolaborasi multipihak, serta penguatan kapasitas kelembagaan.11 Dengan demikian, langkah yang dilakukan BPSDM bisa dinyatakan sebagai fondasi dalam menciptakan tata kelola digital yang inklusif dan berkelanjutan.

D. Tekanan Global dalam Otonomi Lokal

Tekanan global yang semakin menuntut birokrasi untuk melakukan digitalisasi sistem dan perlindungan data publik telah menuntut BPSDM untuk merespon hal tersebut. Maka dari itu, inisiatif yang dilakukan oleh BPSDM merupakan ekspresi dari otonomi lokal yakni kemampuan daerah untuk menginisiasi kebijakan berbasis konteks lokal namun tetap terhubung dengan standar global. Caroline Thomas menyebut fenomena ini sebagai bentuk dari developmental human security, yaitu upaya lokal untuk menjamin keselamatan manusia dalam ekosistem digital yang semakin kompleks dan berisiko.12 Dalam kondisi ini, BPSDM tidak hanya mengisi kekosongan peran, tetapi juga telah memperluas cakupan keamanan

birokrasi dari dimensi teknis menuju dimensi etis dan manusiawi. Selain itu, program seperti Leadership Update Forum yang menghadirkan BSSN dan Kominfo merupakan contoh dari praktik multilayered governance. Hal ini menunjukan bahwa peran otoritas tidak lagi tunggal, melainkan tersebar di antara aktor-aktor dengan fungsi dan kapasitas yang berbeda.13 Konsep ini selaras dengan pendekatan networked

governance, di mana keberhasilan tata kelola tidak ditentukan oleh kekuatan pusat tetapi oleh efektivitas kerja sama antar lembaga.

KESIMPULAN

Dengan demikian, berdasarkan seluruh pembahasan diatas mengenai bagaimana kontribusi BPSDM dalam menangani ancaman kejahatan siber terhadap ASN di era globalisasi. Dapat disimpulkan, bahwa BPSDM Jawa Timur telah menunjukkan kapasitasnya sebagai aktor lokal yang responsif terhadap isu global khususnya dalam menghadapi ancaman kejahatan siber di era digital. Melalui berbagai program edukatif seperti ASN Belajar dan Leadership Update Forum. BPSDM tidak hanya meningkatkan literasi digital para ASN, tetapi juga meninternalisasi norma- norma global seperti zero trust, resilience mindset, dan cognitive triangle ke dalam konteks birokrasi lokal. Keterlibatan komunitas seperti ICSF, serta kolaborasi dengan lembaga nasional seperti BSSN dan Kominfo. Menunjukkan bahwa BPSDM telah aktif dan berkontribusi dalam membangun tata kelola berbasis networked dan multilayered governance. Namun, meskipun BPSDM masih menghadapi sejumlah tantangan baik secara struktural maupun psikososial. BPSDM telah menunjukan upaya untuk mengatasi rendahnya kesadaran digital ASN terhadap ancaman kejahatan siber. Di sisi lain, inisiatif BPSDM juga mencerminkan ekspresi otonomi lokal dalam merespons tekanan global. BPSDM juga telah menjadi bentuk nyata dari developmental human security. Oleh karena itu, upaya BPSDM dapat dipandang sebagai fondasi penting dalam membangun birokrasi yang adaptif, inklusif, dan berkelanjutan di tengah transformasi digital global.

DAFTAR PUSTAKA

Caroline Thomas. 2001. Global Governance, Development and Human Security: The Challenge of Poverty and Inequality. London, Pluto Press. Hal 6

Caroline Thomas. 2001. Global Governance, Development and Human Security: The Challenge of Poverty and Inequality. London, Pluto Press.

Ian Mann. 2008. Hacking the Human: Social Engineering Techniques and Security Countermeasures. Aldershot, Gower Publishing. Hal 2–3 Thomas G. Weiss and Rorden Wilkinson. 2013. International Organization and Global Governance. London: Routledge. Hal 5

Mia Haryati Wibowo dan Nur Fatimah. 2017. "Ancaman Phishing Terhadap Pengguna Sosial Media dalam Dunia Cyber Crime." JOEICT 1. Hal 1–5.

Octo Iskandar. 2024. "Analisis Kejahatan Online Phishing pada Masyarakat." Jurnal Leuser 1, no. 2. Hal 33–35

Russel Butarbutar. 2023. "Kejahatan Siber Terhadap Individu: Jenis, Analisis, dan Perkembangannya." Technology and Economics Law Journal 2. Hal 304–309.

Sandra J. MacLean, David R. Black, and Timothy M. Shaw. 2006. A Decade of Human Security: Global Governance and New Multilateralisms. Aldershot: Ashgate. Hal 3–5

Thomas G. Weiss and Rorden Wilkinson. 2013. International Organization and Global Governance. London: Routledge. Hal 3–5

Thomas G. Weiss and Rorden Wilkinson. 2014. International Organization and Global Governance, 2nd ed. London, Routledge.

Thomas G. Weiss and Rorden Wilkinson. 2014. International Organization and Global Governance, 2nd ed. London, Routledge. Hal 3

Thomas Osburg and Christiane Lohrmann, eds. 2017. Sustainability in a Digital World: New Opportunities Through New Technologies. Cham, Springer.