e-ISSN: 2550-0813 | p-ISSN: 2541-657X | Vol 10 No 7 Tahun 2023 Hal. : 3556-3568

NUSANTARA: Jurnal Ilmu Pengetahuan Sosial

available online http://jurnal.um-tapsel.ac.id/index.php/nusantara/index

URGENSI PENINGKATAN KESADARAN MASYARAKAT TENTANG KASUS PENIPUAN ONLINE BERKEDOK KERJA PARUH WAKTU SEBAGAI ANCAMAN NEGARA

Ihsania Karin Azzani, Susilo Adi Purwantoro, Hikmat Zakky Almubaroq

Prodi Manajemen Pertahanan, Fakultas Manajemen Pertahanan,

Universitas Pertahanan Republik Indonesia

Abstrak

Ancaman terhadap negara yang muncul dari kejahatan dunia maya, terutama dalam bentuk penipuan online yang menggunakan modus pekerjaan paruh waktu, telah menjadi sangat serius. Meskipun kemajuan dalam keterampilan digital yang ditawarkan oleh era teknologi informasi memiliki potensi sebagai alat pemberdayaan, namun juga membuka celah bagi pelaku kejahatan untuk memanfaatkan ketidaktahuan dan kelengahan masyarakat. Tulisan ini membahas dengan rinci mengenai urgensi peningkatan kesadaran masyarakat terkait ancaman yang dihadirkan oleh kejahatan dunia maya, terutama dalam kasus penipuan online yang merangkap sebagai pekerjaan paruh waktu. Melalui pendekatan literasi digital, masyarakat mampu memahami risiko serta teknik manipulatif yang sering kali diterapkan dalam penipuan online. Dampak ancaman ini tidak hanya bersifat ekonomis dengan dampak yang merugikan individu dan sektor bisnis, melainkan juga memiliki potensi mengganggu stabilitas sosial dan kedaulatan negara. Oleh karena itu, keterlibatan pemerintah, lembaga pendidikan, dan sektor swasta dalam memperkuat kesadaran masyarakat terhadap ancaman ini menjadi sangat penting melalui pendidikan, kampanye literasi digital, serta kolaborasi erat antara berbagai pihak, masyarakat dapat menjadi lebih waspada dan berperan aktif, lebih waspada dan cerdas dalam berinteraksi di dunia maya maka perlunya tindakan segera untuk mengatasi ancaman kejahatan dunia maya demi menjaga integritas dan stabilitas negara.

Kata Kunci: Literasi digital, Kesadaran masyarakat, Ancaman negara, Scamming, penipuan online.

*Correspondence Address : Ihsania.broto@mp.idu.ac.id
DOI : 10.31604/jips.v10i7.2023. 3556-3568

PENDAHULUAN

Konsep negara Indonesia merupakan sebagai negara hukum yang melibatkan konsep yang dikembangkan oleh pendirinya yang memiliki arti bagian dari mengatur setiap peraturan tanpa kesewenang-wenangan (Kusniati, 2011), bahwa setiap manusia memiliki hak asasi manusia sejak ia lahir, hal ini dijamin oleh negara dengan berhak berkelangsungan hidup, kepastian hukum, serta pengakuan yang adil dalam bermasyarakat bahwa masyarakat berhak mendapatkan perlindungan dari kekerasan dan diskriminasi yang tertulis pada pasal 28 D ayat 1 pada Undang-Undang Dasar 1945. Perkembangan pesat internet saat ini berdampak besar, tetapi juga membawa masalah serius, yaitu kejahatan dunia maya. Di era modern yang dipenuhi teknologi digital dan internet, penipuan online menjadi masalah serius. Semakin banyaknya penggunaan teknologi ini, pelaku kejahatan dunia maya sangat mudah masuk ke dunia maya untuk mendapatkan keuntungan. Adapun masyarakat yang kurangnya teliti dan kesadaran masyarakat tentang penipuan online menjadi tren saat ini, hal ini memungkinkan para pelaku kejahatan siber merampas keuntungan yang mereka incar hal ini sebagai fenomena yang relatif baru hanya sedikit lembaga penegak hukum yang memiliki kemampuan untuk mengungkapnya secara efektif (Susan W Brenner, 2010).

Dengan semakin mudahnya untuk mengakses penggunaan perangkat teknologi, maka juga semakin mudah untuk memperoleh informasi. Bahkan, kita sebagai masyarakat juga telah mencapai titik di mana kita tengah menghadapi "kebanjiran" informasi, yang berpotensi mengakibatkan tumpang tindih informasi, miskomunikasi bahkan disinformasi. Hal ini belum termasuk dengan terus berkembangnya inovasi dalam teknologi informasi yang semakin canggih yang memudahkan dapat terkoneksi antar individu dengan yang lainya serta membuat pencapaian tujuan individu semakin terfasilitasi. Adanya internet segala kebutuhan manusia dipermudah oleh dengan media digital, dan hal ini semakin ditingkatkan dengan konsep Kecerdasan Buatan *(Artificial Intelligence),* yang membenarkan ungkapan bahwa kita berada dalam zaman *Internet of Things (IoT)* (Yuilista, 2021).

Literasi digital merupakan kunci dan kombinasi dari segi kemampuan membaca dan menulis sebagai pemanfaatan teknologi komunikasi yang canggih untuk keberlangsungan hidup manusia (Sahiruddin, 2021) dan untuk membantu masyarakat aktif dalam menggunakan *smartphone* dan meningkatkan kesadaran mengenai cara menghindari ancaman yang sering terjadi di kalangan masyarakat, khususnya penipuan online yang sedang marak saat ini, penting untuk memahami bahwa kejahatan dunia maya atau *cyber crime* merupakan ancaman serius bagi negara dan masyarakat di era digital saat ini. Kegiatan ilegal ini memanfaatkan kemajuan teknologi telekomunikasi untuk mencari keuntungan atau merugikan pihak lain. (Maskun, 2013) Kesadaran masyarakat terhadap kasus penipuan online masih perlu ditingkatkan, terutama terkait risiko dan taktik yang digunakan oleh para penjahat atau *scammer online* salah satu taktik yang sedang trend saat ini yang diliput Tempo.co bicara fakta menjelaskan dari kasus penipuan online ini adalah salah satu strategi yang digunakan dalam penipuan ini diawali tawaran pekerjaan paruh waktu via aplikasi pesan dengan nomor yang tidak dikenal seperti *WhatsApp* saat menanyakan darimana mendapatkan data pribadi kita, kata mereka dapat dari database calon korban dari portal-portal pekerjaan via online yang ada. Lalu, Penipuan ini dimulai dengan menawarkan pekerjaan

yang sangat sederhana hanya memerlukan tombol "*Like, Follow, Subscrobe dan me Review*" di platform seperti YouTube,Instagram,TikTok dan toko *E-commerce* lainya, selanjutnya korban kemudian dijanjikan komisi sebesar Rp 60.000 apabila mereka berhasil menyelesaikan tiga tugas beruntun dengan menekan tombol tersebut (Febyana Siagian, 2023)

Setelah mencapai kesepakatan, pelaku akan mengundang dan membujuk korban untuk pindah ke dalam grup telegram yang mereka kendalikan dan meminta korban untuk menyelesaikan tugas-tugas tertentu dengan versi lebih banyak. Pada awalnya, pelaku akan memastikan bahwa komisi akan tetap dibayarkan hingga tugas kelima. Namun, setelah beberapa tahap, korban akan diminta untuk mendepositkan sejumlah uang, biasanya minimal Rp 600.000, dengan iming-iming bahwa mereka akan mendapatkan komisi atau bagi hasil sebesar 40% setelah mendepositkan uang tersebut.

Taktik penipuan ini berlanjut dengan merayu korban untuk terus menerus melakukan deposit uang pada tahapan berikutnya, dengan dalih yang sama bahwa mereka akan menerima imbalan yang lebih besar lagi dan korban biasanya baru tersedar bahwa ini penipuan onlin setelah komisi mereka tidak dibayarkan kembali dan telah menyerakhan deposit yang besar para pelaku itu memblock dan menghilang begitu saja yang tidak bisa di hubungi kembali dan tidak tahu untuk melaporkan hal tersebut pada pihak yang berwenang.

Dari kasus penipuan online memiliki konsekuensi yang serius bagi negara karena dampaknya sangat luas dan signifikan, jika dilihat dari segi ekonomi, penipuan online mampu menciptakan kerugian yang substansial, baik bagi individu maupun sektor bisnis, penjahat online juga terlibat dalam berbagai bentuk penipuan lainnya, mulai dari penipuan judi online, penipuan saham, hingga penipuan via e-commerce ini (Tyler Moore, 2009). Selain itu, mereka juga terlibat dalam berbagai jenis kejahatan lainnya, para korban penipuan online sering mengalami kerugian finansial yang substansial, baik itu akibat jatuh ke dalam skema investasi palsu dengan harapan mendapat hasil imbalan yang besar, atau bahkan menjadi korban pencurian identitas.

Pelaku kejahatan ini bahkan menciptakan situs web palsu yang memiliki nama domain mirip dengan platform *e-commerce* yang sebenarnya beroperasi di Indonesia, ancaman terhadap keamanan bisa berasal dari berbagai sumber berdasarkan asalnya, ancaman dapat dikelompokkan menjadi yang berasal dari luar negeri dan yang berasal dari dalam negeri (Budi Raharjo, 1998-2005). Langkah ini meningkatkan potensi kerentanan masyarakat terhadap penipuan online karena situs palsu tersebut mudah dijangkau dan sulit dibedakan dari situs asli. Oleh karena itu, diperlukan usaha lebih lanjut untuk memberikan pemahaman kepada masyarakat mengenai berbagai risiko dan strategi yang digunakan oleh para penipu dalam dunia maya. Dengan meningkatkan tingkat kesadaran dan kewaspadaan, masyarakat dapat lebih siaga menghadapi ancaman penipuan online dan mengurangi peluang menjadi korban dari tindakan kriminal di ranah siber.

Kasus semacam ini memiliki signifikansi yang tinggi bagi negara dan memerlukan partisipasi aktif masyarakat dalam mengembangkan pemahaman tentang literasi digital yang efektif bahwa banyak individu yang merasa dirugikan dan bingung dalam melaporkan insiden penipuan siber kepada lembaga yang memiliki wewenang di Indonesia, kejahatan siber dan penipuan online merupakan salah satu bentuk utama ancaman di ranah digital. Selain itu, dalam tulisan ini akan

diidentifikasi mengapa penipuan online menjadi ancaman serius bagi negara, mengakibatkan kerugian ekonomi yang besar, mengikis kepercayaan publik, dan mengganggu stabilitas sosial. Penipuan online juga memiliki dampak yang lebih luas, hal ini dapat menghancurkan kepercayaan publik terhadap platform digital dan layanan online, merusak hubungan antarindividu dan entitas bisnis serta ketidakstabilan finansial dan emosional. Oleh karena itu, penting bagi negara untuk menghadapi ancaman serius ini dengan serius pula. Langkah-langkah perlu diambil untuk melindungi masyarakat dari penipuan online, termasuk edukasi masyarakat mengenai taktik penipu online, penguatan sistem keamanan siber, dan penegakan hukum yang tegas terhadap para pelaku kejahatan siber.

Scamming cyber crime merujuk pada kegiatan penipuan yang dilakukan melalui media digital, seperti *e-mail*, pesan teks, media sosial, atau situs web palsu. Pelaku kejahatan sering menggunakan manipulasi psikologis, informasi palsu, atau teknik penipuan lainnya untuk memanipulasi korbannya dan meraih keuntungan finansial atau data pribadi (Alfian, 2017) sebai upaya bentuk mengatasi penyebaran yang semakin luas dari kejahatan internet, penting bagi setiap negara dan masyrakat untuk memiliki kesadaran akan potensi penyalahgunaan internet yang berbahaya oleh karena itu, langkah-langkah berikut merupakan cara global dalam menanggulangi masalah ini yaitu : kejahatan digital, termasuk tindak penipuan dalam dunia siber (Ketaren, 2006), telah menjadi ancaman serius di lingkungan digital dengan terus berkembangnya teknologi informasi dan komunikasi, semakin banyak individu yang menggunakan internet untuk berbagai keperluan, seperti transaksi online, komunikasi sosial, dan berbelanja daring. Namun, seiring dengan perkembangan teknologi ini, pelaku kejahatan juga semakin memanfaatkannya untuk melakukan penipuan secara daring dengan metode yang semakin kompleks, inovatif, dan sulit untuk dideteksi.

Hal ini termasuk sebagai kejahatan siber yang melibatkan sejumlah aktivitas kriminal du dunia maya dan platform digital banyaknya bentuk dan jenis kejahatan siber, penipuan online telah menjadi permasalahan yang mengkhawatirkan, dengan modus operandi yang berperan sebagai pekerjaan paruh waktu bagi masyarakat. Penipuan online ini melibatkan praktek manipulatif dengan tujuan menyesatkan individu atau bahkan entitas organisasi untuk memperoleh keuntungan finansial atau informasi pribadi yang memiliki nilai, kebijakan kriminalisasi adalah keputusan kebijakan yang mengubah perilaku yang pada awalnya tidak dianggap sebagai tindak pidana menjadi perbuatan yang dapat dikenakan sanksi pidana (Natsir, 2009).

Dalam upaya menghadapi ancaman ini, penting untuk meningkatkan kesadaran masyarakat tentang taktik penipuan online, mendorong literasi digital, serta mengembangkan kebijakan dan kerjasama yang efektif untuk mengatasi penipuan online sebagai ancaman negara penelitian ini bertujuan untuk menganalisis peran literasi digital dalam meningkatkan kesadaran masyarakat tentang kejahatan dunia maya, khususnya dalam menghadapi kasus penipuan online, serta untuk menyoroti pentingnya upaya pemerintah dan lembaga terkait dalam melindungi masyarakat dari ancaman ini.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan melakukan studi literatur dan analisis terhadap data-data yang relevan dengan topik penelitian. Data dikumpulkan melalui

penelusuran artikel ilmiah, laporan penelitian, studi kasus, dan sumber-sumber terpercaya lainnya yang berhubungan dengan penipuan online dan literasi digital. Hasil penelitian kemudian dianalisis dan disusun menjadi muatan jurnal yang komprehensif. Data yang diperoleh dalam penulisan ini adalah data-data sekunder yang berasal dari studi keputakaan dan studi dokumentasi, bahwa bahan hukum primer yakni bahan hukum yang berasal peraturan perundang-undangan yang berkaitan dengan penyusunan artikel ini, adapun bahan hukum sekunder adalah bahan hukum yang berasal dari buku, jurnal ataupun karya tulis ilmiah yang berkaitan dengan penelitian ini (Soekanto, 2015)

HASIL DAN PEMBAHASAN

Ancaman merujuk pada segala usaha dan kegiatan, baik yang berasal dari dalam maupun luar negeri, yang dianggap memiliki potensi untuk mengancam atau mengganggu kedaulatan negara, integritas wilayah, serta keselamatan seluruh rakyat yang termaktub pada pasal 22 ayat 1 pada Undang-Undang Tentara Nasiona Indonesia Nomor 34 tahun 2004 sementara itu, kejahatan dunia maya, yang juga dikenal sebagai kejahatan siber atau cybercrime, mengacu pada rangkaian tindakan kriminal yang dilakukan melalui internet, jaringan komputer, atau teknologi digital lainnya lalu kita perlu membedakannya menurut Susan W Brenner menjelaskan bahwa Membedakan "kejahatan siber" dari "kejahatan" umumnya melibatkan tindakan yang melanggar norma-norma sosial karena membahayakan kemampuan masyarakat untuk menjaga keteraturan, keteraturan ini tercipta melalui adanya aturan yang melarang berbagai aktivitas dan lembaga "berisiko" yang bertujuan untuk menjaga disiplin serta aturan-aturan ini membentuk dasar dari hukum pidana dalam suatu masyarakat maka, hukum pidana dirancang untuk mencegah masyarakat untuk saling merugikan dengan cara-cara yang mengganggu norma-norma yang ada,cara ini dicapai dengan mengidentifikasi jenis perilaku tertentu yang tidak dapat diterima sebagai "kejahatan" (Susan W Brenner, 2010). Kejahatan memiliki variasi bentuknya karena setiap bentuk menargetkan "kerugian" yang spesifik. Sasaran dari kejahatan bisa berdampak merugikan individu (seperti pembunuhan atau pemerkosaan), hal lainya merugikan properti (seperti pembakaran atau pencurian), merugikan pemerintah (seperti menghalangi proses hukum atau pengkhianatan), dan merugikan moralitas (seperti pelecehan seksual atau perjudian) dalam cakupan ini termasuk berbagai tindakan yang berhubungan dengan penggunaan komputer dan internet yang berpotensi menyebabkan kerugian bagi individu, organisasi, dan bahkan keseluruhan negara.

Kejahatan dunia maya memiliki potensi untuk membahayakan keamanan nasional dan stabilitas negara.

Jenis-jenis kejahatan dunia maya sangat beragam, meliputi:

1. **Penipuan Online /*Cybercrime*:** Ini melibatkan praktik manipulatif untuk mengecoh individu atau organisasi agar memberikan informasi pribadi, keuangan, atau melakukan transaksi yang menguntungkan pelaku kejahatan.
2. **Malware dan Serangan Ransomware:**termasuk penyebaran perangkat lunak berbahaya *(malware)* yang bisa merusak atau mengambil alih sistem komputer, serta serangan ransomware yang mengenkripsi data dan meminta tebusan.

3. **Pencurian Identitas /*Scamming:*** Pelaku mencuri informasi pribadi dan keuangan individu untuk mengakses rekening atau melakukan kegiatan kriminal lainnya atas nama korban.
4. **Pembobolan Data:** Pelanggaran terhadap data pribadi atau bisnis dengan tujuan mencuri informasi sensitif seperti nomor kartu kredit, informasi medis, atau rahasia industri.
5. **Serangan DDoS *(Distributed Denial of Service):*** Serangan yang bertujuan membuat layanan online tidak tersedia dengan cara menghambat akses ke situs web atau layanan melalui aliran lalu lintas internet yang berlebihan.
6. ***Phishing*:** Upaya untuk mendapatkan informasi sensitif dengan menyamar sebagai entitas tepercaya melalui email, pesan instan, atau situs web palsu.
7. **Kejahatan Konten Digital:** Meliputi penyebaran konten ilegal seperti pornografi anak, pembajakan hak cipta, dan penyebaran materi ekstremis atau terorisme.

Ancaman Terhadap Negara:

Ancaman yang ditimbulkan oleh kejahatan dunia maya terhadap negara sangat serius dan beragam. Beberapa aspek penting meliputi:

1. **Keamanan Nasional:** Kejahatan siber dapat mengancam infrastruktur kritis, sistem pertahanan, dan komunikasi nasional, membuka celah bagi serangan siber yang merusak dan mengganggu hal ini untunk mengembangkan kemampuan strategis negara dalam beroperasi pertahanan negara (Cahyadi, 2016).
2. **Spionase dan Pencurian Data Sensitif:** di mana pihak-pihak seperti negara lain atau kelompok dengan niat jahat berusaha untuk mencuri informasi yang sensitif dan bernilai, seperti rahasia negara, data intelijen, dan informasi militer. Upaya ini bertujuan untuk memperoleh keuntungan strategis, politik, atau ekonomi atas negara yang menjadi target (Hidayati, 2022). Pencurian data sensitif seperti ini dapat mengakibatkan kerugian yang serius, merusak keamanan nasional, serta mengancam kedaulatan dan stabilitas negara tersebut. Oleh karena itu, upaya pencegahan dan perlindungan terhadap spionase serta pencurian data sensitif merupakan hal penting dalam menjaga keamanan siber negara.
3. **Gangguan Politik dan Sosial:** Penyebaran informasi palsu dan propaganda online dapat mempengaruhi opini publik, memicu konflik politik penyebaran hoaks politik akan mengganggu stabilitas sosial (Qardini, 2022).
4. **Krisis Ekonomi:** Serangan siber terhadap lembaga keuangan atau bisnis dapat mengakibatkan kerugian finansial yang signifikan dan bahkan menciptakan krisis ekonomi.
5. **Pembobolan Data Pribadi:** Pencurian data pribadi masyarakat atau pejabat pemerintahan dapat membahayakan privasi dan

mengancam integritas sistem pemerintahan.

Mengenai pengaturan pemidanaan kejahatan dunia maya di Indonesia, sebagian besar kegiatan kejahatan dunia maya di negara ini belum diatur secara jelas oleh peraturan hukum secara khusus dalam undang-undang yang ada, maka ketika terjadinya akan menangani kasus kejahatan dunia maya, kerangka hukum melibatkan penggunaan ketentuan yang terkandung dalam KUHP (Koto, 2021) dan undang-undang lain di luar ruang lingkup KUHP, Ketentuan KUHP sering diterapkan dengan interpretasi yang sangat luas untuk menuntut pelaku kejahatan dunia maya, dalam hal ini, ketentuan yang berkaitan dengan tindak pidana penipuian online atau scamming termasuk yang dapat diperluas untuk mencakup tindak pidana dunia maya.

Dengan meningkatnya kompleksitas dan intensitas kejahatan dunia maya, negara-negara perlu mengembangkan kebijakan, kerja sama internasional, dan upaya pencegahan yang efektif untuk melindungi keamanan dan stabilitas nasional penelitian menunjukkan bahwa saat mengunakan media digital sebagai alat untuk berinteraksi di dunia maya ataupun digital tetap memakai aturan serta diberlakukan norma yang berlaku di masyarakat (Bambang Yuniarto, 2021) literasi digital juga memainkan peran penting dalam meningkatkan kesadaran masyarakat tentang kejahatan dunia maya, khususnya penipuan online untuk menjadi melek pada kasus cyber crime / kejahatan dunia maya juga merupakan dasar, karena kejahatan dunia maya ini merupakan masalah serius dan bagaimana fundamental individu itu sendiri sebagai sifat dasar pengetahuan dan bagiamana pribadi bisa melihat cara pandang yang berbeda yang mungkin akan lebih kolefktif, aktif serta cermat saat bagaimana pribadi itu mengkomunikasikan pengetahuan via media digital (Julian McDougall, p. 266) dengan memiliki pemahaman tentang ancaman yang mungkin terjadi secara online, masyarakat dapat mengenali taktik penipuan yang umum digunakan dan mengambil langkah-langkah pencegahan yang tepat. Dalam penelitiannya, Klara menguraikan bahwa secara lebih terperinci, literasi diartikan sebagai "kemampuan menggunakan teknologi digital dan perangkat komunikasi, serta jaringan untuk mengakses, mengelola, mengintegrasikan, mengevaluasi, menciptakan, dan mengkomunikasikan informasi dengan tujuan berpartisipasi dalam masyarakat berbasis pengetahuan (Klara Nelson M. C., 2011). Hal ini dijelaskan bahwa literasi digital memiliki dimensi pengetahuan terhadap praktik-praktik keamanan online, termasuk penggunaan kata sandi yang kuat, melakukan verifikasi keamanan pada situs web, serta pencegahan terhadap upaya *phishing,* selain itu, penelitian ini menekankan signifikansi pendekatan kolaboratif dalam meningkatkan literasi digital di kalangan masyarakat dengan kerjasama antara lembaga pendidikan, pemerintah, organisasi non-pemerintah, dan penyedia layanan internet menjadi esensial untuk menyediakan program-program literasi digital yang efektif dan dapat dijangkau oleh semua segmen masyarakat. Inisiatif ini dapat diwujudkan melalui pelatihan, workshop, serta kampanye sosial yang bertujuan untuk meningkatkan kesadaran masyarakat mengenai ancaman kejahatan siber dan cara untuk menghindarinya serta pentingnya akan peningkatan kesadaran masyarakat tentang kejahatan dunia maya melalui literasi digital dapat berperan penting dalam menghadapi kasus penipuan online. Literasi digital memberikan pemahaman yang lebih baik tentang risiko dan taktik penjahat online, serta membantu masyarakat dalam mengenali

dan menghindari skema penipuan dengan modus yang sama.

Selain itu, penelitian ini juga menyoroti peran pemerintah dan lembaga terkait dalam melindungi masyarakat dari ancaman penipuan online melalui penyediaan pendidikan literasi digital yang efektif, pengembangan kebijakan yang memperkuat perlindungan konsumen, dan penegakan hukum yang tegas terhadap pelaku kejahatan dunia maya.

Kejahatan Dunia Maya Dan Ancaman Terhadap Negara

Ancaman negara adalah segala usaha dan aktivitas, baik yang berasal dari dalam negeri maupun luar negeri, yang dianggap memiliki potensi mengganggu atau merugikan kedaulatan negara, integritas wilayah negara, dan keselamatan seluruh warganya. Bahwa Peran Pemerintah Indonesia dalam Melindungi Negara dari ancaman penipuan online yang sedang trend di tahun 2023, meliputi berbagai aspek yang penting dalam meningkatkan perlindungan terhadap negara dari penipuan online, berikut adalah penjelasan yang lebih detail mengenai peran pemerintah dan langkah-langkah yang dapat diadopsi untuk melindungi negara:

1. **Pembentukan Lembaga Keamanan Siber**: Pemerintah dapat memainkan peran penting dalam melindungi negara dari penipuan online dengan membentuk lembaga keamanan siber yang bertanggung jawab untuk mengidentifikasi, mencegah, dan menanggapi serangan siber. Lembaga ini akan memiliki sumber daya dan keahlian yang diperlukan untuk mendeteksi ancaman penipuan online, memperkuat infrastruktur digital negara, dan memberikan respons yang cepat dan efektif terhadap serangan yang terjadi.
2. **Penegakan Hukum yang Ketat:** Pemerintah dapat mengadopsi kebijakan penegakan hukum yang ketat terhadap pelaku penipuan online. Hal ini mencakup peningkatan kerjasama antara aparat penegak hukum dan lembaga keamanan siber untuk menyelidiki dan menindak pelaku penipuan online, harus memastikan adanya hukuman yang memadai bagi pelaku penipuan online guna memberikan efek jera dan mencegah penipuan di masa mendatang.
3. **Kerjasama Internasional dalam Pertukaran Informasi:** Ancaman penipuan online bersifat lintas batas dan seringkali melibatkan jaringan internasional. Oleh karena itu, pemerintah Indonesia perlu menjalin kerjasama internasional dengan negara-negara lain dalam pertukaran informasi tentang penipuan online. Ini termasuk pertukaran data tentang taktik penipuan, serangan siber yang terdeteksi, dan praktik terbaik dalam melindungi negara dari ancaman serupa. Kerjasama internasional ini akan membantu meningkatkan pemahaman dan respons kolektif terhadap penipuan online.
4. **Strategi Peningkatan Kesadaran Masyarakat melalui Literasi Digital:** Pemerintah dapat

mengadopsi strategi yang fokus pada peningkatan kesadaran masyarakat melalui literasi digital dalam menghadapi penipuan online. Ini melibatkan pelaksanaan program edukasi dan kampanye publik yang meningkatkan pemahaman masyarakat tentang taktik penipuan online, mengenali tanda-tanda penipuan, dan cara melindungi diri dari ancaman tersebut. Pemerintah juga dapat mempromosikan pendidikan literasi digital di tingkat pendidikan formal dan non-formal, serta melibatkan sektor swasta dan lembaga masyarakat dalam upaya ini.

5. **Kolaborasi dengan Pihak Swasta dan Lembaga Masyarakat:** Pemerintah dapat berkolaborasi dengan pihak swasta dan lembaga masyarakat dalam upaya melindungi negara dari penipuan online. Ini mencakup keterlibatan perusahaan teknologi, penyedia layanan keuangan, dan lembaga keuangan dalam mengimplementasikan langkah-langkah keamanan digital yang ketat. Pemerintah juga dapat memfasilitasi kerjasama dengan lembaga masyarakat, seperti asosiasi konsumen, kelompok advokasi, dan lembaga pendidikan untuk mengembangkan program literasi digital yang efektif.

Langkah-langkah dengan harapan upaya yang komprehensif serta negara dapat meminimalkan risiko dan dampak penipuan online, serta menciptakan lingkungan digital yang lebih aman bagi masyarakat dan negara.

Dalam menghadapi ancaman penipuan online yang marak terjadi peran pemerintah Indonesia memegang peranan penting dalam melindungi negara dan masyarakat. selain itu, masyarakat juga harus selalu siap untuk melaporkan kasus awal kepada pihak berwenang yang terdekat, khususnya ke kepolisian daerah. laporan-laporan ini memiliki signifikansi besar karena jika diabaikan atau tidak diselidiki, mereka dapat membawa dampak yang berbahaya, terutama menghadapi ancaman di masa depan.

Ketika kejahatan tidak dilaporkan dengan memadai, hal ini menyebabkan terbatasnya upaya investigasi dan urgensi dari pihak penegak hukum dan penuntutan. Jika masalah ini tidak terangkat dalam statistik dan kasus yang diberitahukan atau diselidiki, dampaknya akan terus diabaikan saat prioritas ditetapkan, yang berdampak signifikan pada alokasi anggaran dalam perencanaan masa mendatang (Buono, 2014).

Hingga saat ini, usaha dalam menganalisis kejahatan dunia maya dan memahami potensi masalah yang muncul, sehingga ancaman di masa yang akan datang bisa diidentifikasi dan rekomendasi prioritas bisa diusulkan, sangatlah penting. mengingat adanya faktor-faktor pendukung kejahatan dunia maya yang baru muncul dengan motif yang sama, hal ini menjadi dasar yang esensial. Semua ini menjadi pondasi bagi pembuat kebijakan dan hukum untuk mengkaji kembali atau memperkenalkan instrumen dan alat baru guna mengatasi tantangan yang muncul.

Strategi meningkatkan kesadaran masyarakat melalui literasi digital seperti ini menjadi langkah krusial dalam menghadapi tantangan penipuan online / cybercrime di Indonesia pada tahun 2023. dengan cara

ini, masyarakat akan diberikan pemahaman mendalam mengenai penipuan online serta melalui pendidikan digital, pengembangan kampanye penyadaran, implementasi pendidikan literasi digital di lingkungan pendidikan, kerja sama erat dengan sektor swasta dan partisipasi masyarakat aktif yang turut andil untuk menyadari pentingnya untuk selalu berhati-hati dengan semua modus penipuan yang ada, serta pembelajaran dari pengalaman negara lain dalam penanggulangan serupa, diharapkan bahwa dengan upaya ini, tingkat kesadaran masyarakat Indonesia terhadap ancaman penipuan online/ *cybercrime* dapat ditingkatkan secara signifikan.

Melalui peningkatan kesadaran ini, individu akan lebih terampil dalam mengenali dan menghindari skema penipuan online, sehingga mereka dapat melindungi diri sendiri serta kontribusi positif bagi keseluruhan komunitas.

Mencegah Kejahatan Dunia Maya Sebagai Ancaman Negara Melalui Analisis Srategis Dan Literasi Digital

Dalam era globalisasi dan kemajuan ilmu pengetahuan serta teknologi yang pesat, perlindungan negara dari berbagai bentuk ancaman menjadi prioritas utama, ancaman ini melibatkan tidak hanya komponen militer, tetapi juga meliputi faktor nonmiliter dengan tingkat kerumitan yang beraneka ragam. Ancaman yang bersifat nirmiliter bisa melibatkan dimensi ideologi, politik, ekonomi, budaya sosial, teknologi, informasi, dan juga keselamatan publik (A'raf, 2015) Untuk menjaga keunggulan kompetitif negara, penting bagi pemerintah serta masyarakat untuk memahami konsep bela negara yang melibatkan segala aspek kehidupan. Masyarakat, terutama generasi milenial, perlu diberdayakan dengan pemahaman tentang pentingnya bela negara sebagai cinta tanah air, pemahaman tentang negara Indonesia, dan kesadaran yang berkelanjutan tentang kekuatan Pancasila sebagai ideologi bangsa (Komala, 2018) dalam upaya melindungi negara dari ancaman yang termasuk di dalamnya kejahatan siber, peran literasi digital memiliki peran yang sangat signifikan dalam menjaga kelangsungan dan mendalami aspek-aspek tersebut.

Dalam usaha mencegah ancaman kejahatan dunia maya terhadap negara, ada dua pendekatan utama yang dapat diambil: yaitu analisis strategis dan literasi digital. (1)Pendekatan analisis strategis merupakan serangkaian insiden kejahatan siber yang terjadi di Indonesia, stabilitas keamanan dan ketertiban nasional sedang menghadapi ancaman sangat nyata, meningkatnya tingkat eskalasi kejahatan siber telah mencapai taraf yang signifikan, namun menangani tindakan yang melanggar hukum di dunia maya tidaklah mudah dengan hanya mengandalkan kerangka hukum yang sudah ada hal ini disebabkan oleh hubungan yang rumit di antara lima faktor kunci yang mencakup pada : pelaku kejahatan, korban kejahatan, reaksi sosial terhadap kejahatan, serta sistem hukum (Edy Soesanto, 2023).

Dalam konteks ini, pendekatan analisis strategis menjadi krusial dalam usaha melindungi keamanan negara dari ancaman kejahatan dunia maya. Pendekatan ini melibatkan identifikasi dan pemahaman mendalam mengenai beragam bentuk ancaman yang mungkin mengganggu negara.

Cara mengadopsi pendekatan analisis strategis ini, negara dapat secara efektif menghadapi ancaman yang berasal dari dunia maya, memperkuat keamanannya, dan membangun perlindungan yang lebih kokoh terhadap kerentanan-kerentanan yang ada.

Di sisi lain, (2) pendekatan literasi digital dalam penguasaan literasi

sangat penting dalam era di mana kehidupan manusia dipengaruhi oleh teknologi informasi, yakni literasi digital pada dasarnya, memiliki literasi digital mengimplikasikan kemampuan untuk memahami cara memanfaatkan informasi dalam bentuk digital (Chusnu Syarifa Diah Kusuma, 2022) melibatkan upaya pendidikan masyarakat mengenai risiko dan taktik yang digunakan dalam kejahatan dunia maya, edukasi dan peningkatan kesadaran akan membantu meningkatkan kemampuan masyarakat dalam mengenali taktik seperti phishing dan ransomware dan cara mahami data individu dan menjaga detail pribadi berfungsi sebagai dasar untuk evolusi masyarakat menuju merangkul norma-norma digital: "Literasi digital mencakup keterampilan untuk mengakses, menangani, memahami, menggabungkan, berkomunikasi, menilai, dan menghasilkan informasi dengan aman dan tepat menggunakan teknologi digital, memungkinkan kemampuan kerja, pekerjaan yang bermakna, dan upaya kewirausahaan. Ini mencakup keahlian yang sering disebut sebagai literasi komputer, literasi TIK, literasi informasi, dan literasi media (Klara Nelson, 2011). Etika digital juga menjadi fokus, dengan mengajarkan perilaku bijak dan bertanggung jawab dalam menggunakan teknologi. Penggunaan alat keamanan digital juga diajarkan, termasuk penggunaan antivirus dan manajemen kata sandi yang kuat (Wilkie, 2011)

Kerjasama antara pemerintah, lembaga pendidikan, sektor swasta, dan masyarakat menjadi kunci dalam menerapkan kedua pendekatan ini. Melalui analisis strategis, negara dapat mengidentifikasi potensi ancaman dan risiko yang ada, sementara dengan meningkatkan literasi digital pada masyarakat, kerentanan terhadap ancaman dunia maya dapat dikurangi, dan kesadaran akan pentingnya etika digital dan pemahaman teknologi dapat ditanamkan.

Peningkatan pemahaman terhadap literasi digital dalam memanfaatkan internet secara bijak dan bertanggung jawab, dan hal ini juga menjadi pertimbangan penting bagi pemerintah pusat, dan ini juga diperlukan dalam kerangka pelaksanaan Undang-Undang Republik Indonesia nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik serta Undang-Undang nomor 14 tahun 2008 tentang Keterbukaan Informasi Publik. Dua undang-undang ini menangani aspek manajemen dan perlindungan informasi serta data dalam transaksi elektronik serta akses informasi publik. Prinsip-prinsip yang diatur dalam undang-undang ini memberikan pijakan penting bagi Pemerintah dalam menjamin kepastian hukum.

Upaya meningkatkan literasi digital tidak hanya berfokus pada kelompok tertentu, tetapi melibatkan semua kalangan masyarakat, pada konsep *good governance* salah satu upaya yaitu meningkatkan literasi digital tidak hanya berfokus pada kelompok tertentu saja, tetapi melibatkan semua kalangan masyarakat. Tidak hanya masyarakat umum, tetapi juga para pejabat publik perlu memiliki tingkat literasi digital yang memadai guna meningkatkan efisiensi dan transparansi dalam pelaksanaan tugas mereka, literasi digital juga memiliki peran krusial dalam reformasi birokrasi, sebagai upaya strategis untuk mencegah praktik kolusi, korupsi, dan nepotisme, dengan tujuan mewujudkan tata kelola pemerintahan yang lebih baik / *good governnace* (Kurnia, 2021).

Pemahaman tentang semangat bela negara meliputi pentingnya keamanan siber dan perlindungan data dari serangan cybercrime dalam rangka menjaga integritas negara. Peran masyarakat dalam melaporkan perilaku mencurigakan dan dalam kampanye

literasi digital sangat penting untuk tujuan ini. Keamanan siber mencerminkan kesiapan berkorban demi menjaga kemerdekaan, kedaulatan, persatuan, dan kesatuan negara. Ini melibatkan upaya pencegahan serta tindakan proaktif dalam menghadapi ancaman kejahatan siber yang dapat mengganggu stabilitas negara dan masyarakat.

KESIMPULAN

Studi kejahatan siber dan ancaman siber sangat penting untuk mengatasi risiko yang ditimbulkan oleh terorisme digital. Individu dapat menggunakan pengetahuan dan keterampilan untuk mengidentifikasi dan mencegah kejahatan siber. Namun, mengatasi ancaman cyber membutuhkan perencanaan strategis dan kolaborasi antara berbagai stakeholder untuk mencapai kesuksesan dalam terorisme digital di dalam komunitas.

Dengan menerapkan penggunaan internet yang positif dan proaktif, berfokus pada pencegahan kejahatan siber, dan memastikan ketersediaan informasi yang dapat diandalkan dan dapat dipercaya, masyarakat dapat menjadi lebih sadar dan mengambil langkah-langkah aktif untuk melindungi diri dari ancaman siber.

Aspek pertama dan paling penting dari pencegahan kejahatan siber adalah menangani masalah cybercrime hal ini melibatkan menangani masalah kejahatan siber dengan menangani kebutuhan masyarakat dan memastikan bahwa pemerintah, pendidikan, dan pemangku kepentingan lainnya bekerja sama untuk mengembangkan program literasi digital yang efektif. Kerjasama internasional dalam informasi dan praktek juga penting untuk mengatasi kejahatan siber.

Dalam memahami risiko yang terkait dengan terorisme digital dan kejahatan siber sangat penting untuk mengatasi tantangan yang dihadapi masyarakat. Dengan menerapkan strategi yang efektif dan mendorong kolaborasi antara pemangku kepentingan, potensi kejahatan siber dan ancaman siber dapat dikurangi secara signifikan.

DAFTAR PUSTAKA

Alfian, M. (2017). PENGUATAN HUKUM CYBER CRIME DI INDONESIA DALAM PERSPEKTIF . *Kosmik Hukum*, 152.

A'raf, A. (2015). Dinamika Keamanan Nasional. *Jurnal Keamanan Nasional* , 33.

Bambang Yuniarto, R. P. (2021). LITERASI DIGITAL SEBAGAI

PENGUATAN PENDIDIKAN KARAKTER. *Edueksos: Jurnal Pendidikan Sosial dan Ekonomi Vol 10, No 2*, 179.

Budi Raharjo. (1998-2005). *Keamanan Sistem Informasi.* Jakarta: PT Insan Infonesia - Bandung & PT INDOCISC.

Buono, L. (2014). Fighting cybercrime through prevention, outreach and awareness raising. . *In ERA Forum (Vol. 15, No. 1, pp. 1-8). Berlin/Heidelberg: Springer Berlin Heidelberg*, 165.

Cahyadi, I. (2016). TATA KELOLA DUNIA MAYA DAN ANCAMAN KEDAULATAN NASIONAL. *Jurnal Politica dinamika masalah politik dalam negeri & hubungan Internasional*, 221.

Chusnu Syarifa Diah Kusuma, R. I. (2022). Strengthening of Digital Literacy to Support Student Community Service to Prevent Hoax and Cybercrime. In 9th International Conference on Education Research, and Innovation (ICERI 2021). *Atlantis Press* , 482.

Edy Soesanto, A. R. (2023). Analisisdan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. *SAMMAJIVA : Jurnal Penelitian Bisnisdan Manajemen*, 188.

Febyana Siagian. (2023). *Waspada Penipuan Kerja Paruh Waktu dengan Penghasilan Lumayan, Begini Modusnya* . Jakarta: Temopo.Co https://metro.tempo.co/read/1748548/waspada-penipuan-kerja-paruh-waktu-dengan-penghasilan-lumayan-begini-modusnya .

Hidayati, A. R. (2022). Penegakan Hukum Privasi pada Aktivitas Perdagangan Elektronik. *Repository Digital Universitas Al Azhar Indonesia*, 24.

Julian McDougall, M. R. (Vol 43, No 3 2018). The uses of (Digital) Literacy. *Learning, Media and Technologhy*, 266.

Ketaren, E. (2006). CYBERCRIME, CYBER SPACE, DANCYBER LAW. *Jurnal TIMES Vol 5 No 2* , 40.

Klara Nelson, M. C. (2011). Teaching Tip An Investigation of Digital Literacy Needs of Students. *Ais Elibrary Nelson, K., Courier, M., & Joseph, G. W. (2011Journal of Information Systems Education, 22(2), 95-110.*, 96.

Klara Nelson, M. C. (2011). Teaching Tip An Investigation of Digital Literacy Needs of Students . *Journal of Information Systems Education*, 98.

Komala, M. d. (2018). MEMBANGUN KESADARAN BELA NEGARA BAGI GENERASI MILENIAL. *Jurnal Pemikiran dan Penelitian Manajemen Pertahanan* , 70.

Kurnia, D. (2021). NALISIS KRITIS TERHADAP GERAKAN NASIONAL LITERASI DIGITAL DALAM PERSPEKTIF GOOD GOVERNANCE. *Jrnal Academia Praja Volume 4 Nomor 1*, 112.

Kusniati, R. (2011). Sejarah Perlindungan Hak Asasi Manusia dalam kaitannya dengan konsepsi negara hukum. *INOVATIF Jurnal ilmu hukum*, 79.

Maskun. (2013). *Kejahatan Siber (Cyber Crime) suatu pengantar* . Jakarta: Kharisma Putra Utama.

Natsir, N. I. (2009). KEBIJAKAN KRIMINAL TERHADAP TINDAK PIDANA. *(Doctoral dissertation, UNIVERSITAS DIPONEGORO).*, 45.

Qardini, L. (2022). PENGUATAN LITERASI BERINTERNET SEHAT DAN CERDAS KEPADA MASYARAKAT DESA PAMBOBORANGKECAMATAN BANGGAE KABUPATEN MAJENEMENUJU DESA SEHAT INTERNET. *Jurnal Pengabdian masyarakat lembaga penelitian dan pengabdian masyarakat universistas pahlawan tuanku tambusai Vol 3 no 3*, 1478.

Sahiruddin. (2021). *Pengembangan Literasi Membaca dan Menulis di Era Digital* . Malang: Media Nusa Creative.

Soekanto, S. (2015). *Penelitian Hukum Normatif suatu tinjauan singkat.* Jakarta : Rajawali Pers.

Susan W Brenner. (2010). *Cybercrime Criminal Threats From Cyberspace.* United States America: Greenwood Publishing Group.

Susan W Brenner. (2010). *Cybercrime Criminal Threats From Cyberspace.* United States of America: Greenwood Publishing Group.

Tyler Moore, R. C. (2009). The Economics of Online Crime. *Journal of Economic Perspectives, 23(3), 3-20.*

Wilkie, S. M. (2011). Information security activities of college students: An exploratory study. *Academy of Information and Management Sciences Journal, 14(2), 91-116.*, 19.

Yuilista, Y. (2021). The Urgency of Digital Media Literacy Education to Increase Digital Proficiency Leve. *Sustainable Jurnal Kajian Mutu Pendidikan* , 3.