MIMBAR KEADILAN
MKJIH

Perkembangan Cybercrime : Dampak Terhadap Keamanan dan Ketahanan Nasional serta Pencegahannya

Vice RLYS[1], Natalya Christine Simaremare[2], Sahata Manalu, SH., M.[3]

[1,2,3]Program Studi Ilmu Hukum FH Universitas Katolik Santo Thomas Sumatera Utara
Vicer4770@gmail.com

Abstract

Cyber crime merupakan ancaman nyata terhadap keamanan dan ketahanan nasional karena dampaknya yang semakin meluas seiring berjalannya kompleksitas teknologi informasi. Kejahatan internet ini dapat mengganggu stabilitas ekonomi, politik, dan sosial bahkan dapat membahayakan infrastruktur vital negara. Untuk mencegah ancaman cyber, upaya untuk penanggulangan dan pencegahan sangat penting. Hal ini termasuk meningkatkan infrastruktur keamanan, meningkatkan kesadaran masyarakat akan resiko cyber crime, dan meningkatkan penegakan hukum dan untuk memberikan sanksi yang tegas kepada pelaku cyber crime.

Keywords

Cybercrime; Pencegahan; Keamanan; Ketahanan Nasional

Introduction

Berkembangnya globalisasi dan kemajuan teknologi informasi telah mengubah kehidupan individu. Teknologi informasi membuat masyarakat dengan mudah dan cepat dapat menerima dan memberikan informasi kepada masyarakat luas. Proses pergeseran keadaan di seluruh dunia yang ditandai dengan kemajuan teknologi dan informasi yang menimbulkan saling ketergantungan dan pengaburan di luar batas negara yang dikenal sebagai globalisasi. Selain memiliki dampak positif, teknologi informasi juga memiliki dampak negatif, yaitu memungkinkan untuk melakukan Cybercrime. Cybercrime adalah tindakan kriminal yang memanfaatkan teknologi komputer dan jaringan internet untuk melakukan kejahatan. Perbuatan ini merupakan perbuatan yang melanggar hukum dan tindakan yang menimbullkan ancaman dan kerugian.

Menurut Golose (2006) modus kejahatan cybercrime dibagi ke dalam beberapa bentuk berdasarkan bentuk sesuai modus operasinya seperti berikut:

1) Unauthorized Access to Computer System and Service, yaitu akses tidak sah mengacu pada tindakan memasuki sistem komputer atau jaringan tanpa izin dari pemiliknya. Tindakan ini dapat dilakukan dengan berbagai metode, termasuk teknik hacking, penggunaan malware, atau pencurian kredensial pengguna.
2) Illegal Contents, yaitu mencakup semua jenis informasi atau materi yang melanggar hukum, seperti pornografi anak, materi yang bersifat kebencian, penipuan, dan informasi yang dapat membahayakan keamanan publik

3) Data Forgery, yaitu tindakan untuk membuat atau mengubah informasi digital dengan maksud menipu orang lain. Ini dapat meliputi dokumen keuangan, identitas, atau data penting lainnya.
4) Cyber Espionage, yaitu praktik mengumpulkan informasi rahasia dari individu atau organisasi lain melalui teknologi internet. Tindakan ini sering dilakukan oleh perusahaan untuk meraih keuntungan kompetitif atau oleh negara untuk tujuan intelijen.
5) Cyber Sabotage and Extortion, yaitu melibatkan penghancuran atau pengacauan data dan sistem komputer dengan tujuan merusak operasi suatu organisasi. Sementara itu, pemerasan siber terjadi ketika pelaku meminta uang tebusan untuk tidak merusak data atau sistem.
6) Offense against Intellectual Property, yaitu pelanggaran yang terjadi ketika seseorang menggunakan karya cipta orang lain tanpa izin, seperti mendistribusikan musik, film, perangkat lunak, atau paten tanpa lisensi yang sah.
7) Infringements of Privacy, yaitu tindakan mengakses atau menggunakan informasi pribadi seseorang tanpa izin. Ini dapat mencakup pencurian identitas dan pengungkapan data pribadi secara tidak sah.
8) Cracking,yaitu proses membobol sistem keamanan komputer dengan tujuan mencuri data atau merusak sistem. Tindakan ini sering dilakukan oleh hacker untuk mendapatkan akses ke perangkat lunak berbayar secara gratis.
9) Carding,yaitu praktik menggunakan informasi kartu kredit orang lain secara ilegal untuk melakukan transaksi tanpa sepengetahuan pemilik kartu tersebut. Ini biasanya dilakukan melalui forum gelap di internet.

Hal ini terjadi karena keamanan dan ketahanan nasional dalam sebuah negara semakin sensitif terhadap adanya serangan cyber crime yang semakin mengganggu seiring perkembangan zaman yang terus berkembang. Serangan ini tidak hanya menimbulkan ancaman pada infrastruktur vital, tetapi juga dapat mengganggu stabilitas politik, mengambil data sensitif dari individu, perusahaan, bahkan negara, dan mencuri privasi dan keamanan individu. Pemerintah, lembaga internasional, dan sektor swasta di seluruh dunia sudah sangat memperhatikan dampak cyber crime pada keamanan dan ketahanan nasional, khususnya di Indonesia.

Kementerian Komunikasi dan Informatika (Kominfo) mengemukakan bahwa serangan Cyber crime terus meningkat dan mengancam lebih dari 10 juta identitas. Pada tahun 2014, serangan ini sudah berdampak kepada 11 juta identitas, kemudian naik menjadi 13 juta identitas pada 2015, dan 15 juta identitas pada 2016. Kominfo juga menyatakan bahwa Indonesia termasuk dalam daftar 10 besar negara yang menjadi target serangan siber di dunia. Dari sepuluh negara yang ditargetkan, Indonesia berada di urutan kelima atau keenam.

Menurut laporan Symantec dalam Internet Security Threat Report tahun ini, Indonesia mengalami peningkatan serangan terhadap jaringan internet secara global. Pada 2015, Indonesia berada di peringkat ke-29, namun pada 2016 naik ke peringkat ke-17. Selain itu, surat elektronik yang mengandung perangkat lunak perusak juga meningkat, dari 1 dalam 236 email pada awalnya menjadi 1 dalam 156 email. Laporan Akamai State of the Internet Security untuk triwulan pertama 2017 menunjukkan bahwa Indonesia berada di peringkat ke-17 dalam hal serangan melalui 3,2 juta permintaan laman berbahaya yang diterima oleh pelanggannya. Para penyerang tertarik dengan data penggunaan internet di Indonesia yang menunjukkan potensi perputaran uang dalam jumlah besar, yang mendorong mereka untuk berusaha mendapatkan keuntungan dari serangan tersebut.

Penting bagi hukum Indonesia untuk dapat berkembang bersamaan dengan perubahan sosial dan teknis. Aturan hukum dapat dibuat lebih efektif dan efisien dengan dukungan teknologi, terutama digitalisasi. Masyarakat memerlukan proses hukum yang lebih cepat,

transparan, dan lebih mudah diakses, serta sistem hukum Indonesia perlu mengadopsi teknologi digital untuk mengikuti perubahan budaya dan substansi. (Putra, 2020)

Penulisan ini akan membahas berbagai aspek penting dari dampak cybercrime terhadap keamanan dan ketahanan nasional. Selain itu, akan dibahas juga berbagai metode penanggulangan yang telah diterapkan oleh pemerintah. Diharapkan jurnal ini akan meningkatkan pemahaman kita tentang ancaman cybercrime terhadap keamanan dan ketahanan nasional, serta dapat membantu pembuatan kebijakan dan praktik terbaik untuk mencegah serangan cyber di masa depan.

Methodology

Dalam penelitian ini, tinjauan pustaka digunakan untuk menelaah dan menganalisis karya-karya tulis atau literatur yang relevan dengan topik yang sedang diteliti. Metode ini bertujuan untuk memperoleh pemahaman yang lebih mendalam mengenai topik tertentu, mengkaji temuan-temuan penelitian sebelumnya, serta menyusun kerangka teoretis yang kokoh untuk penelitian yang akan dilakukan (Fink, 2019). Peneliti mencari literatur terkait topik penelitian mereka dari berbagai sumber, seperti jurnal, buku, artikel, dan dokumen daring. Dalam hal ini, penulis membatasi topik penelitian pada kejahatan siber yang ditemukan melalui database Google Scholar. Keunggulan akses terbuka yang disediakan oleh database ini, yang memudahkan proses pengumpulan data, menjadikannya pilihan utama.

Selanjutnya, penulis membaca dan mempelajari tinjauan yang ada, mencatat informasi yang relevan, serta mengorganisasi data dengan cara yang sistematis. Setelah itu, penulis menganalisis data dari tinjauan tersebut dan menyusun sintesis atau rangkuman hasilnya. Pada tahap akhir, penulis menyusun laporan penelitian dengan menggabungkan hasil analisis yang telah dilakukan. Penulis memilih metode tinjauan pustaka karena memiliki berbagai keuntungan, antara lain kemampuan untuk mengakses informasi yang luas dari berbagai bidang, efisiensi waktu dan biaya, serta dapat dijadikan referensi dalam penulisan karya ilmiah.

Discussion

Perkembangan Teknologi di Indonesia

Perkembangan masyarakat saat ini ditandai oleh proses industrialisasi yang didukung oleh kemajuan teknologi telekomunikasi. Hal ini mendorong hubungan antarnegara menjadi lebih mendunia, menciptakan tatanan global yang baru. Dalam konteks ini, Indonesia sebagai negara yang sedang membangun di era reformasi tidak dapat menghindari pengaruh tersebut. Berbagai krisis, baik di bidang politik, ekonomi, maupun sosial budaya, dihadapi oleh masyarakat Indonesia dan memerlukan penanganan yang serius. Agar bangsa dan negara Indonesia tetap diakui dan dihargai keberadaannya di antara bangsa-bangsa di dunia, tantangan-tantangan ini harus diatasi dengan baik.

Perkembangan teknologi informasi dan komunikasi telah membawa keberadaan internet sebagai tantangan sekaligus peluang dalam berbagai aspek kehidupan, mengingat tingginya minat masyarakat Indonesia terhadap penggunaan internet. Pada awal tahun 2023, jumlah pengguna internet di Indonesia tercatat mencapai 212,9 juta, mengalami peningkatan dibandingkan dengan periode yang sama tahun sebelumnya.

Berdasarkan data yang dirilis oleh We Are Social, total populasi Indonesia pada Januari 2023 adalah 276,4 juta, dengan 49,7% di antaranya perempuan dan 50,3% pria. Dari jumlah tersebut, 212,9 juta orang merupakan pengguna internet, yang menunjukkan kenaikan sebesar

5,2% atau sekitar 10 juta pengguna dibandingkan dengan tahun 2022. We Are Social juga melaporkan bahwa rata-rata waktu yang dihabiskan pengguna internet Indonesia setiap hari adalah 7 jam 42 menit. Penggunaan internet di Indonesia mayoritas dilakukan melalui perangkat gadget, dengan rata-rata waktu penggunaan 4 jam 53 menit, sementara penggunaan komputer dan tablet hanya sekitar 2 jam 49 menit. Untuk media sosial, We Are Social mencatat bahwa 167 juta orang di Indonesia atau sekitar 60,4% populasi menggunakan platform seperti Facebook, Instagram, TikTok, dan lainnya.Telah terlihat adanya peningkatan jumlah pengguna internet di Indonesia maupun di seluruh dunia setiap tahunnya.

Keberhasilan pembangunan nasional sangat bergantung pada ketahanan nasional yang didukung melalui pemberdayaan masyarakat. Ketahanan ini menciptakan keadaan di mana gangguan dan ancaman, termasuk kejahatan, dapat dihindari. Dengan seiring dengan kemajuan ilmu pengetahuan dan teknologi, perkembangan kejahatan pun turut mengalami transformasi. Kini, kejahatan tidak lagi dilakukan secara tradisional; para pelakunya memanfaatkan berbagai peluang yang ditawarkan oleh alat-alat modern dan teknologi canggih.

Kejahatan jenis ini dikenal sebagai kejahatan berdimensi baru, yang mencerminkan perubahan dalam masyarakat, terutama di bidang perekonomian dalam konteks industri. Pelakunya sering kali berasal dari kalangan terdidik, mampu, dan terorganisasi, termasuk dalam kategori kejahatan kerah putih (white collar crime).

Selain itu, mobilitas kejahatan saat ini sangat tinggi, tidak terbatas pada satu wilayah, melainkan dapat melintasi batas-batas regional hingga transnasional. Modus operandi kejahatan ini menggunakan teknologi mutakhir dan memanfaatkan kelemahan dalam sistem hukum dan manajemen. Korban kejahatan pun menjadi lebih kompleks, tidak hanya individu, tetapi juga kelompok masyarakat dan bahkan negara. Parahnya, banyak korban yang tidak segera menyadari telah dirugikan oleh tindakan tersebut (Kunarto, 1991:2).

Dampak Cyber Crime Terhadap Ketahanan dan Keamanan Nasional

Dampak kejahatan siber terhadap keamanan nasional tidak dapat diremehkan. Serangan siber berpotensi menciptakan kerentanan pada infrastruktur penting, seperti sistem keuangan, kesehatan, dan energi. Akibatnya, hal ini dapat mengganggu layanan publik, menyebabkan kebocoran data sensitif, bahkan yang paling serius adalah mendapatkan sabotase terhadap operasi militer dan intelijen. Selain itu, serangan yang dilancarkan oleh negara asing atau kelompok terorganisir dapat mengancam kedaulatan dan posisi negara, serta memicu konflik internasional. Jika dijelaskan lebih rinci, kejahatan siber dapat mempengaruhi keamanan nasional dalam berbagai aspek, sebagai berikut:

A. Menargetkan Infrastruktur Kritis

   Kejahatan siber dapat berpotensi melumpuhkan infrastruktur kritis seperti jaringan listrik, penyediaan air, dan sistem transportasi, yang pada gilirannya dapat menyebabkan kekacauan dan kerusakan yang parah. Salah satu contoh yang mencolok adalah serangan ransomware WannaCry pada tahun 2017, yang menyebabkan gangguan pada komputer di rumah sakit, bank, dan perusahaan di seluruh dunia. Ketidakstabilan pada infrastruktur kritis ini dapat mengancam keselamatan publik, merusak perekonomian, serta memicu konflik sosial.

B. Mencuri Data Sensitif

   Kejahatan siber juga dapat mengakibatkan pencurian data sensitif, termasuk data pemerintah, informasi keuangan, dan data pribadi. Data-data ini dapat disalahgunakan untuk tujuan kriminal seperti penipuan identitas, pemerasan, atau bahkan kegiatan spionase. Kebocoran data sensitif ini bisa merusak kepercayaan publik terhadap pemerintah dan institusi, serta memberikan dampak negatif terhadap reputasi negara di kancah internasional.

C. Menyebarkan Propaganda dan Disinformasi
Kejahatan siber sering dimanfaatkan untuk menyebarkan propaganda dan disinformasi, yang berpotensi menimbulkan kerusuhan sosial, merusak stabilitas politik, serta mencoreng citra negara. Sebagai contoh, pada tahun 2016, terdapat tuduhan bahwa intervensi siber dilakukan untuk memengaruhi hasil pemilihan presiden Amerika Serikat.

D. Mengganggu Layanan Publik
Keberadaan kejahatan siber dapat berdampak negatif pada layanan publik, termasuk situs web pemerintah, layanan e-government, serta sistem perbankan. Hal ini berpotensi menghalangi akses masyarakat terhadap layanan penting dan mengganggu aktivitas ekonomi. Gangguan terhadap layanan publik dapat memicu frustrasi dan kemarahan di kalangan masyarakat, yang pada gilirannya dapat merusak kepercayaan publik terhadap pemerintah.

E. Mengintimidasi dan Membungkam Suara Kritis
Kejahatan siber sering digunakan sebagai alat untuk mengintimidasi dan membungkam suara-suara kritis, seperti jurnalis, aktivis, dan pembela hak asasi manusia. Praktik ini berujung pada penyempitan ruang publik dan demokrasi, serta menghambat kemajuan sosial

Contoh Kasus Cyber Crime di Indonesia

Berikut adalah beberapa contoh kasus kejahatan siber di Indonesia yang sangat meresahkan dan menarik perhatian dunia maya:

1. Pencurian Data Bank Syariah Indonesia (BSI) pada Mei 2023, salah satu server Bank Syariah Indonesia (BSI) mengalami kerusakan parah selama lima hari, menyebabkan para nasabah tidak dapat mengakses aplikasi mobile banking mereka. Kelompok hacker asal Rusia, Lockbit, mengklaim bertanggung jawab atas gangguan tersebut. Mereka juga mengaku telah mencuri data sebanyak 1,5 terabyte, termasuk data pribadi nasabah dan pegawai bank. Selain itu, mereka mengancam pihak bank untuk membayar sejumlah uang agar data tersebut dapat dipulihkan, atau jika tidak, data akan dijual di dark web. Kasus ini tercatat sebagai salah satu serangan ransomware terbesar di Indonesia (amt.it, 2023).
2. Pembobolan Data oleh Hacker Bjorka pada tahun 2022, banyak kasus kejahatan siber yang mencuri data pribadi, salah satunya oleh hacker Bjorka, yang sempat viral karena berhasil membobol data milik Bank Indonesia (BI) pada Januari 2022. Setidaknya ada tujuh kasus besar yang dilakukan oleh Bjorka pada tahun tersebut. Data yang berhasil dibobol termasuk registrasi kartu SIM milik Kominfo, data nasabah Bank Indonesia, data pasien rumah sakit, pelamar Pertamina, pelanggan PLN, pelanggan Jasa Marga, dan lainnya. Bjorka lebih sering menargetkan perusahaan dengan sistem keamanan server yang lemah (amt.it, 2023).
3. Modus Penipuan Melalui File APK di WhatsApp, modus penipuan online dan peretasan yang menggunakan malware melalui file APK (Android Package) sempat marak. Para pelaku kejahatan siber menipu korban dengan berbagai modus lewat WhatsApp, meminta korban untuk membuka dan menginstal file APK yang berisi malware guna mencuri data dan uang korban. Perusahaan keamanan siber ITSEC Asia mengungkapkan bahwa metode seperti sniffing dan phishing sering digunakan oleh para hacker. Sniffing adalah teknik untuk memantau dan meretas data sensitif seperti kredensial, password, dan PIN melalui jaringan internet.

Modus penipuan ini sering kali menyamar sebagai undangan pernikahan, informasi perbankan, pengecekan resi pengiriman, cek data BPJS atau asuransi, dan bahkan foto barang yang dibeli secara online. Menurut Divisi Humas Polri, kerugian yang diakibatkan oleh kasus sniffing ini diperkirakan mencapai 12 miliar rupiah, dengan sekitar 483 orang menjadi korban (liputan6.com).

Pada tahun 2024, Indonesia mengalami lonjakan signifikan dalam jumlah insiden kejahatan siber. Menurut laporan dari SAFEnet, tercatat 61 insiden keamanan digital pada kuartal pertama tahun ini, hampir dua kali lipat dibandingkan dengan periode yang sama pada tahun 2023, yang hanya mencatatkan 33 insiden. Peningkatan ini setara dengan tambahan 28 insiden dibandingkan tahun sebelumnya, dengan rata-rata insiden bulanan pada 2023 sebesar 11, sedangkan pada 2024 meningkat menjadi 16,25 insiden per bulan. Beberapa insiden besar termasuk serangan ransomware yang melibatkan 130 serangan, serta 4.046 serangan phishing yang menargetkan sektor layanan informasi dan infrastruktur kritis. Menjelang Pemilu 2024, ancaman kejahatan siber terus meningkat, dengan motif politik menjadi salah satu faktor utama di balik serangan digital tersebut.

Beberapa faktor yang turut mendorong meningkatnya kasus kejahatan siber antara lain anonimitas di dunia digital, kemajuan teknologi yang mempermudah pelaku dalam melaksanakan kejahatannya, kesenjangan sosial yang memotivasi individu untuk terlibat dalam cybercrime, insentif finansial, kelalaian pengguna komputer, mudah dilakukan dengan resiko keamanan yang kecil, tidak diperlukan peralatan yang super modern. Pada dasarnya, para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu yang besar, dan fanatik terhadap teknologi komputer, sistem keamanan jaringan yang lemah dan kurangnya kontrol masyarakat dari penegak hukum (Anwar, 2011). Di samping itu, penegakan hukum terhadap kejahatan siber juga terhambat oleh keterbatasan sumber daya dan kemampuan teknologi yang dimiliki oleh aparat penegak hukum.

Kejahatan siber terus berkembang seiring dengan pesatnya kemajuan teknologi digital. Hal ini dapat merugikan korban, baik secara finansial maupun nonfinansial. Kemajuan di bidang informasi dan teknologi tidak selalu memberikan dampak positif bagi negara atau masyarakat, karena seringkali dampak positif tersebut diikuti oleh dampak negatif. Kemajuan tersebut terkadang justru menjadi lahan subur bagi berkembangnya kejahatan, terutama dalam hal Cybercrime. Cybercrime juga dikenal sebagai kejahatan dunia maya, yaitu berupa kejahatan yang dilakukan dengan menggunakan teknologi informasi dan komunikasi sebagai objek atau sasaran dari kejahatan tersebut. Cybercrime termasuk kejahatan terhadap kerahasiaan, integritas, dan ketersediaan informasi (Rowe,2019).

Efek Penggunaan Internet Terhadap Stabilitas Keamanan

Menurut data (Kompas, 2021) terdapat beberapa contoh efek dari penggunaan internet terhadap stabilitas keamanan dalam negeri Indonesia, antara lain:

a. Kasus BPJS Kesehatan

Pada akhir Mei 2021, situs Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, yakni bpjs-kesehatan.go.id diduga diretas. Hasilnya, Forum Raid diduga membocorkan data milik 279 juta warga Indonesia. Data yang termasuk NIK, nomor telepon, alamat, dan gaji dijual seharga 0,15 bitcoin, atau sekitar 84,4 juta rupiah pada 20 Mei 2021. Kajian menyeluruh yang dilakukan oleh Kementerian Komunikasi dan Informasi menemukan bahwa data sampel dari dataset tersebut tampaknya mirip dengan data BPJS Kesehatan. Akhirnya, Kementerian Komunikasi dan Informatika mengusulkan untuk menghapus tautan untuk mengunduh data pribadi. Ini termasuk memblokir Forum Raid sebagai tindakan proaktif untuk mencegah penyebaran data lebih lanjut.

b. Kasus Asuransi BRI Life
Bisnis asuransi BRI Life didirikan pada 27 Juli 2021. Dalam kasus ini, diperkirakan 2 juta data nasabah BRI Life bocor dan dijual secara online seharga U$D 7.000, atau sekitar Rp 101,6 juta (kurs 21 Juli 2021). Akun Twitter pertama kali mengungkapkan kebocoran data.

@UnderTheBreach mengatakan bahwa pencuri berhasil mengambil 250 GB data BRI Life, termasuk 2 juta file PDF data pelanggan dan sekitar 463 ribu dokumen lainnya. Informasi seperti gambar KTP, rekening, nomor wajib pajak, akte kelahiran, dan rekam medis termasuk dalam data nasabah yang bocor. Ada kemungkinan bahwa kebocoran data terjadi karena pihak yang tidak bertanggung jawab menggunakan celah keamanan dalam sistem elektronik internal BRI Life.

c. Situs Sekretariat Kabinet Republik Indonesia
Beberapa hari kemudian, metode deface digunakan untuk diretas halaman web Sekretariat Kabinet Republik Indonesia (Setkab RI) setkab.go.id. Secara sederhana, metode ini memungkinkan peretas mengubah tampilan halaman web tujuan sesuai dengan tujuannya. Situs setkab.go.id diretas pada 30 Juli 2022. Situs tersebut berubah tampilannya menjadi hitam dan menampilkan foto para demonstran membawa bendera merah putih dengan keterangan "Padang Blackhat || Anon Illusion Team Owned By Zyy Ft Luthfifake." Polisi percaya bahwa peretasan ini dilakukan untuk keuntungan finansial, dengan maksud untuk menjual script backdoor dari situs web target kepada orang yang membutuhkannya. Menurut penyelidikan sementara polisi, kelalaian operator dan kegagalan sistem keamanan menyebabkan peretasan. Tidak ada dokumen rahasia yang ditemukan di situs web Setkab.

d. Kasus e-HAC Kementerian Kesehatan
Kabar tentang peretasan aplikasi Electronic Health Alert (e-HAC) yang dikembangkan oleh Kementerian Kesehatan (Kemenkes) pada bulan Agustus 2021 mengatakan bahwa data milik 1,3 juta orang Indonesia yang tersimpan di dalamnya telah bocor. e-HAC adalah versi aplikasi modern dari kartu peringatan kesehatan dan diperlukan bagi semua orang yang bepergian, baik di dalam maupun di luar negeri. Peneliti keamanan siber VPNMentor pertama kali menemukan kebocoran data pada 15 Juli 2021. VPNMentor mengatakan bahwa aplikasi e-HAC tidak memiliki protokol keamanan aplikasi yang tepat, sehingga rentan terhadap peretasan dan penyusupan. Menurutnya, pengembang diberitahu menggunakan basis data Elasticsearch yang tidak aman untuk menyimpan data mereka, yang melibatkan data tes Covid-19 penumpang.

e. Badan Intelijen Nasional dan 10 Jaringan Kementerian
Sebuah kelompok peneliti keamanan siber yang berafiliasi melaporkan pada September 2021 bahwa sistem jaringan internal sepuluh kementerian dan lembaga negara Indonesia, termasuk yang dimiliki oleh Badan Intelijen Negara (BIN), diretas. dengan kelompok media internasional TheRecord, Insikt Group hanya mengungkapkan bahwa insiden peretasan terkait dengan Mustang Panda, kelompok hacker asal China yang biasanya memata-matai dunia maya dan berfokus pada wilayah Asia Tenggara. Insikt Group menemukan bahwa server Command and Control (C&C) grup Mustang Panda menggunakan malware jenis PlugX, yang

berhubungan dengan beberapa host yang dapat terinfeksi di jaringan internal pemerintah Indonesia.

f. Situs Pusmanas Badan Siber Sandi Negara
Pada Oktober 2021, hacker menggunakan teknik deface untuk membobol situs milik Badan Siber dan Sandi Negara (BSSN). Pusat Malware Nasional (Pusmanas), yang menurut BSSN berisi informasi tentang laporan malware. Akun Twitter @son1x777 mengunggah serangan terhadap situs BSSN, yang menunjukkan bahwa situs Pusmanas BSSN telah dihack dengan teknik deface, dengan tulisan "Hacked by theMx0nday (diretas oleh theMx0nday)" di halaman muka. BSSN segera menangani kejadian tersebut, yang dilakukan oleh Tim Penanganan Kejadian Keamanan Computer (CSIRT) BSSN.

g. Database Polri
Pada November 2021, pencuri mengklaim telah membobol database Polri; informasi ini diungkapkan oleh akun Twitter @son1x666 pada 17 November 2021. Dalam sebuah tweet, Hacker mengatakan bahwa 28.000 log in dan kredensial pribadi telah dicuri. Selain itu, dia menyertakan tiga tautan yang menunjukkan bahwa data sensitif seperti nama lengkap, tempat tanggal lahir, nomor registrasi pokok, alamat rumah, pangkat, golongan darah, satuan kerja, suku, email, dan pelanggaran yang pernah dilakukan oleh anggota dikumpulkan dari database Polri. Ada juga data seperti identitas propam, data rehabilitasi putusan, keterangan rehabilitasi, dan putusan sidang. Data dapat diakses dan diunduh tanpa biaya.

h. Bjorka
Tahun 2022 dikejutkan dengan sosok Bjorka. Dia diduga seorang hacker yang meretas situs Kementerian Komunikasi dan Informasi. Nama Bjorka muncul dalam komentar yang dia buat sejak Agustus lalu, situs forum brached.to telah dikaitkan dengan peretasan data di Indonesia. Menurut Björka, dia telah menjual 105 juta data warga Indonesia yang diperoleh dari Komisi Pemilihan Umum (KPU). Dia juga menyatakan bahwa dia memiliki 1,3 milyar data pendaftaran kartu SIM prabayar yang terdiri dari operator seluler, nomor telepon, dan NIK (Bineksari, 2022). Beberapa contoh di atas menunjukkan bahwa kemungkinan cybercrime terus meningkat didorong oleh penggunaan internet yang semakin meningkat tanpa pelatihan. Oleh karena itu, pemerintah Indonesia harus mencari komponen perlindungan diri berbasis cyber. Oleh karena itu, pemerintah Indonesia harus memiliki program keamanan cyber yang bertujuan untuk memberikan rasa aman dari serangan cyber.

Cybersecurity

Menurut CISCO, cybersecurity adalah praktik melindungi kerahasiaan (rahasia), integritas (integritas), dan ketersediaan (ketersediaan) informasi di dunia maya. ISO/IEC 27032:2012 menyatakan bahwa cybersecurity adalah upaya yang dilakukan untuk menjaga kerahasiaan (rahasia), integritas (integritas), dan ketersediaan (ketersediaan) informasi di dunia maya, program, sistem, dan jaringan yang terkena serangan digital. Dengan demikian, dapat disimpulkan bahwa keamanan siber, juga dikenal sebagai cybersecurity, adalah suatu tindakan yang melindungi sistem komputer dari serangan atau akses yang tidak sah (Permatasari, 2022).

Menurut jurnal (Yanuar, 2021), terdapat konsep global cybersecurity untuk menangani serangan siber. Global Cybersecurity didasarkan pada lima bidang kerja: Pertama, komponen kepastian hukum (undang-undang tentang kejahatan cyber). Kedua, komponen teknis dan

tindakan prosedural (tindakan konkrit untuk menanggulangi cyberattack), ketiga, komponen struktur organisasi (tindakan konkrit untuk menanggulangi cyberattack), dan keempat, komponen peningkatan kapasitas dan pendidikan pengguna (kampanye dan pendidikan publik tentang keamanan cyber). Kelima, komponen kerja sama internasional, yang mencakup kolaborasi resiprokal dalam upaya mengatasi ancaman cyber.

Metode yang Digunakan Untuk Mengatasi Ancaman Cyber

Hingga saat ini, pemerintah Indonesia telah melakukan berbagai upaya untuk dapat mengatasi ancaman-ancaman yang terjadi. Menurut jurnal (Ardiyanti, 2014) metode yang digunakan oleh negara kita untuk mengatasi ancaman keamanan cyber yaitu sebagai berikut:

a. Kepastian Hukum

Kebijakan keamanan siber di Indonesia dimulai pada tahun 2007 dengan diterbitkannya Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M.Kominfo/5/2007 mengenai Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Peraturan ini kemudian mengalami revisi melalui Peraturan Menteri Komunikasi dan Informatika No. 16/PER/M.KOMINFO/2010 dan pembaruan selanjutnya dengan Peraturan Menteri Komunikasi dan Informatika No. 29/PER/M.KOMINFO/2010. Salah satu hal yang diatur dalam peraturan ini adalah pendirian ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure), yang diberikan tugas oleh Menteri Komunikasi dan Informatika untuk membantu memantau keamanan jaringan telekomunikasi berbasis protokol internet.

Hasyim Gautama menjelaskan bahwa dasar hukum kebijakan keamanan siber Indonesia saat ini berlandaskan pada Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012, serta Surat Edaran Menteri dan Peraturan Menteri.

b. Teknis dan tindakan procedural

Sebagai bagian dari komponen kedua ini, yaitu teknis dan tindakan prosedural, setiap pihak yang terlibat dalam keamanan informasi harus mengambil tindakan nyata dan mematuhi standar infrastruktur yang diperlukan. Adanya pertahanan militer yang memadai, adanya sistem pengawasan jaringan, sistem manajemen informasi dan peristiwa yang mengawasi berbagai kejadian jaringan yang terkait dengan masalah keamanan, dan perangkat keamanan jaringan yang berfungsi sebagai pengendali dan pemeliharaan keamanan.

c. Struktur Organisasi

Kementrian Pertahanan telah membentuk Tim Kerja Pusat Operasi Dunia Maya untuk meningkatkan keamanan cyber. Tujuan dari Cyber Defence Operation Centre adalah untuk menjaga keamanan dan perlindungan keamanan internal (Kemhan) dan keamanan eksternal, yaitu negara Indonesia. Dalam tugas keamanan cyber, pusat tersebut ditugaskan untuk membangun sistem pertahanan yang melibatkan seluruh bagian negara seperti warga negara, wilayah, dan sumber daya untuk menegakkan kedaulatan negara, keutuhan wilayah, dan integritas nasional.

d. Capacity building

Konstruksi kapasitas TNI memainkan peran yang sangat penting dalam meningkatkan kapasitas SDM. TNI sebagai pilar utama keamanan. Dalam hal keamanan cyber, kami telah bekerja sama dengan pihak berwenang di bidang teknologi informasi, seperti Institut Teknologi Del di Sumatera Utara. Tiga program menggambarkan kerja sama ini: persiapan model perang cyber; seminar tentang intelijen dan operasi cyber militer; dan cyber camp atau pekan.

e. Kerjasama Internasional
Indonesia bekerja sama dengan negara lain dalam penanggulangan cybercrime, termasuk bekerja sama dengan negara lain di bidang tertentu seperti Jepang, Inggris, Amerika Serikat, dan beberapa lainnya, serta menjadi anggota berbagai komunitas, organisasi, dan forum internasional, termasuk ASEAN Network Security Action Council, International Telecommunication Union (ITU), Forum of Incident Response and Security (FIRST), dan steering committee Asia Pacific Computer Emergency Response Team (APCERT).

Lima hal tersebut telah dilakukan oleh Badan Siber dan Sandi Negara (BSSN). Namun, hasil pemantauan BSSN, yang memantau dan menemukan potensi serangan siber selama 24 jam penuh setiap hari, mencatat 1,6 milyar serangan siber selama tahun 2021.
siber (Kompas, 2022), menunjukkan bahwa Indonesia masih menjadi salah satu negara yang paling rentan terhadap serangan siber.

Strategi Pencegahan melalui Penegakan Hukum dengan Mengacu pada Undang-Undang.

1. Undang-Undang Negara Republik Indonesia Tahun 1945
UUD 1945 adalah landasan hukum dasar bagi bangsa Indonesia, berperan penting dalam menyelesaikan berbagai tantangan dan mewujudkan cita-cita nasional. Penegakan UUD 1945 secara tepat menjadi kunci utama dalam mencapai tujuan tersebut, khususnya dalam mencegah tindakan kejahatan siber. Berikut adalah beberapa strategi yang dapat diterapkan dalam penegakan hukum berdasarkan UUD 1945
   a. Penguatan Lembaga Penegak Hukum
      - Meningkatkan kapasitas dan profesionalisme kinerja aparat penegak hukum, seperti Polri, Kejaksaan, dan KPK, untuk menegakkan hukum secara adil, transparan, dan akuntabel.
      - Membangun sistem peradilan yang independen dan memiliki integritas tinggi, bebas dari intervensi politik serta kepentingan pribadi.
   b. Peningkatan Kesadaran Hukum Masyarakat
      - Melakukan edukasi hukum secara rutin kepada masyarakat mengenai bahaya dan risiko kejahatan siber.
      - Mendorong masyarakat untuk aktif berpartisipasi dalam penegakan hukum, melalui berbagai program patroli bersama serta laporan ketika terjadi kasus kejahatan siber.
      - Membangun budaya hukum yang kuat di masyarakat dengan menanamkan kesadaran akan pentingnya menghormati hukum dan norma-norma sosial, sehingga dapat mencegah munculnya pelaku kejahatan.
   c. Pembenahan Regulasi dan Perundang-undangan Oleh Aparat Hukum
      - Melakukan evaluasi dan revisi terhadap peraturan perundang-undangan yang sudah tidak relevan, tumpang tindih, atau tidak sesuai dengan tujuan UUD 1945.
      - Menjamin keselarasan antara peraturan perundang-undangan tingkat pusat dan daerah untuk menghindari tumpang tindih dan interpretasi yang beragam.
      - Mengajak partisipasi publik dalam proses legislasi agar peraturan yang dihasilkan dapat mencerminkan kebutuhan dan aspirasi masyarakat.

   d. Penegakan Hak Asasi Manusia (HAM)

- Memastikan bahwa setiap proses penegakan hukum, mulai dari penyelidikan, penyidikan, penuntutan, hingga peradilan, selalu mengedepankan unsur-unsur HAM.
- Memberikan perlindungan hukum kepada korban kejahatan siber dan memastikan mereka mendapatkan akses yang adil terhadap keadilan.
- Mencegah pelanggaran HAM, seperti kejahatan dunia maya, dengan memperkuat mekanisme pencegahan serta pemulihan hak-hak korban.

e. Penegakan Supremasi Hukum
- Menjamin bahwa penegakan hukum dilakukan secara adil dan tanpa diskriminasi, termasuk terhadap aparat penegak hukum, pejabat publik, dan kelompok-kelompok berpengaruh.
- Memastikan akses yang setara terhadap hukum bagi seluruh individu, tanpa memandang perbedaan suku, agama, ras, golongan, atau status sosial ekonomi.
- Memberikan tindakan tegas kepada pelaku kejahatan siber dengan sanksi yang adil dan proporsional.

f. Pemanfaatan Teknologi Informasi dan Komunikasi (TIK)
- Menggunakan teknologi informasi dan komunikasi (TIK) untuk memberikan pengetahuan kepada masyarakat tentang cara menghindari dan menangani kejahatan dunia maya
- Membangun sistem pelaporan pelanggaran hukum secara online yang mudah diakses dan secepat mungkin mendapatkan respons
- Memanfaatkan media sosial untuk menyebarkan informasi hukum dan edukasi kepada masyarakat, sehingga pelaku kejahatan merasa terancam dan mempertimbangkan kembali niat mereka.

Conclusion

Indonesia saat ini berada dalam situasi mendesak mengenai keamanan dunia maya atau cyber-security karena menyaksikan kenyataan bahwa tingkat kejahatan di dunia maya atau cybercrime di Indonesia telah mencapai tahap yang sangat memperihatinkan. Salah satu fakta yang menunjukkan bahwa cybercrime di Indonesia sudah dalam keadaan mengkhawatirkan adalah data CIA yang menyatakan bahwa kerugian yang ditimbulkan akibat tindak kejahatan yang memanfaatkan maupun di dunia cyber di Indonesia telah mencapai 1,20% dari tingkat kerugian akibat cybercrime yang terjadi di seluruh dunia.

Dalam tataran kebijakan, penangganan cybercrime berbeda dengan penangganan kejahatan lainnya. Namun berbeda dengan penangganan kejahatan lainnya, cyber-security membutuhkan pemikiran yang komprehensif untuk menangganinya. Karena itu tulisan ini membahas dua hal yaitu: dampak dari cybercrime terhadap ketahanan dan keamanan negara serta cara penanggulangannya.

Kebijakan keamanan siber yang telah diterapkan di Indonesia telah dimulai sejak tahun 2007 dengan dibentuknya Indonesia Security Incident Response Team on Internet Infrastructure, yang merupakan Tim yang ditugaskan oleh Menteri Komunikasi dan Informatika (Kominfo) untuk membantu pengawasan keamanan jaringan telekomunikasi yang berbasis protokol internet.

Kerangka hukum cyber-security di Indonesia saat ini disusun antara lain berdasarkan UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah mengenai Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012 serta surat edaran menteri dan peraturan menteri. Secara nasional, terdapat berbagai tantangan yang terkait dengan pembangunan cyber-security yang kuat, di antaranya adalah rendahnya pemahaman penyelenggara negara mengenai keamanan terkait dunia cyber yang membutuhkan pembatasan penggunaan layanan yang servernya berada di luar negeri dan diperlukan penggunaan sistem yang aman; belum adanya legalitas yang memadai terhadap penanganan serangan di dunia.

Berdasarkan tulisan di atas, penulis menyimpulkan bahwa ancaman cybercrime terhadap keamanan nasional dapat memiliki dampak besar di Indonesia. Pertama, kejahatan siber dapat mengancam stabilitas nasional dengan mengganggu infrastruktur vital seperti keuangan, transportasi, dan energi. Kedua, pencurian data sensitif oleh pelaku kejahatan siber dapat mengungkap informasi rahasia atau merusak kepentingan negara. Cybercrime juga dapat digunakan untuk spionase dan sabotase yang bertujuan untuk merusak sistem atau infrastruktur penting negara. Untuk melindungi keamanan nasional dari ancaman ini, penegakan hukum harus meningkatkan kerjasama internasional dan meningkatkan kemampuan untuk mendeteksi, menyelidiki, dan menuntut pelaku cybercrime secara efektif. Penegakan hukum di Indonesia dapat memainkan peran penting dalam pembuatan strategi penanggulangan terhadap kasus ini.

Indonesia telah membuat rencana untuk menghadapi dan menanggulangi cybercrime dengan menciptakan kepastian hukum, tindakan teknis dan prosedural yang nyata, struktur organisasi cyber-security, dan meningkatkan kapasitas sumber daya manusia melalui pengembangan kapasitas, kerjasama internasional dengan berbagai kelompok dan hubungan cyber bilateral dengan berbagai negara. Namun demikian, karena Indonesia masih termasuk dalam kategori negara yang rentan terhadap serangan siber, masih kurang efektif dan efisien.

Berdasarkan penjelasan di atas, penulis ingin memberikan beberapa saran untuk mengatasi tantangan ini, sebagai berikut:

1. Peningkatan penegakan hukum perlu dilakukan dengan memperkuat kapasitas sumber daya, baik melalui pelatihan dan pendidikan bagi petugas penegak hukum, maupun dengan merumuskan undang-undang yang sesuai dengan perkembangan teknologi dan tren kejahatan siber yang baru muncul.
2. Penting untuk menjalin kolaborasi antara pemerintah dan sektor swasta guna melindungi infrastruktur kritis serta berbagi informasi terkait ancaman yang mungkin timbul di masa depan.
3. Publik juga harus lebih sadar akan ancaman kejahatan siber, yang seharusnya didorong melalui kampanye edukasi dan sosialisasi.

Dengan pendekatan yang holistik dan kolaboratif seperti ini, diharapkan penegakan hukum akan menjadi lebih efektif dalam melindungi keamanan nasional dari ancaman kejahatan siber yang semakin kompleks..

References

Ardiyanti, H. (n.d.). Cyber security dan Tantangan Pengembangannya di Indonesia. Politica Vol. 5 No. 1 Juni 2014.

Bineksari, R. (2022, November 21). Siapakah Bjorka Hacker Yang Bikin Pemerintah RI Ketar Ketir?

Dewi Chirzah, R. A. (n.d.). CYBER WAR: ANCAMAN PADA KEAMANAN NASIONAL. Jurnal Trends. Volume 01 Tahun 2013.

Dwi Shinta Wati, S. N. (2024). Dampak Cyber Crime Terhadap Keamanan NAsional dan Strategi Penanggulangannya : Ditinjau Dari Penegakan Hukum. Jurnal Bevinding Vol 02 No 01 Tahun 2024.

Kolonel Inf Sugeng Santoso, S. (2018). Memperkuat Pertahanan Siber Guna Meningkatkan Ketahanan Nasional. JURNAL KAJIAN LEMHANNAS RI.

Supanto. (n.d.). PERKEMBANGAN KEJAHATAN TEKNOLOGI INFORMASI (CYBER CRIME) DAN ANTISIPASINYA DENGAN PENAL POLICY. Yustisia. Vol. 5 No. 1 Januari - April 2016.