JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 2 No: 4, Agustus – September 2025
E-ISSN : 3046-4560

PENCEGAHAN DAN TANTANGAN DALAM MEMERANGI TINDAK PIDANA SIBER

PREVENTION AND CHALLENGES IN COMBATTING CYBER CRIME

Nurfitri Fathonah[1], Hudi Yusuf[2]
Fakultas Hukum Universitas Bung Karno
Email: ffsoekadji20@gmail.com[1], hoedydjoesoef@gmail.com[2]

Article Info

Article history :
Received : 15-08-2025
Revised : 17-08-2025
Accepted : 19-08-2025
Pulished : 21-08-2025

Abstract

Throughout 2024, the National Police managed to uncover 325,150 cases in Indonesia throughout 2024. This figure decreased compared to 2023. One of the crimes in the digital era is cybercrime. The digital era that continues to develop rapidly today, namely the internet and information technology has become an important part of everyday life. This development is also inseparable from the emergence of cybercrime known as Cybercrime emerging as a new problem along with technological developments and having serious consequences both at the individual and collective levels. This research is a qualitative research with descriptive methods or techniques. The results of this study are that the National Police admit that it is not easy to prosecute cybercrime criminal cases. The handling is different from other criminal cases. Cybercrime is a crime that uses the internet as a space or place to commit the crime. As for what law enforcement officers do, there are several actions taken in preventing cybercrime by conducting cyber patrols, cyber education, direct warnings via social media, direct action in the form of social media takedowns, law enforcement. One of the biggest challenges is the speed of technology that exceeds the development of existing regulations, creating security gaps that can be exploited by cybercriminals. However, the biggest challenge may lie in the limited number of experts in the field of cybersecurity. The demand for security professionals far exceeds the availability, so many organizations have difficulty protecting their infrastructure from digital threats.

Keywords: Cybercrime, Prevention, Challenges

Abstrak

Sepanjang 2024, Polri berhasil mengungkap 325.150 kasus di Indonesia sepanjang 2024. Angka tersebut menurun dibandingkan dengan tahun 2023. Salah satu kejahatan di era digital adalah kejahatan siber. Era digital yang terus berkembang pesat saat ini, yaitu berupa internet dan teknologi informasi telah menjadi bagian penting dari kehidupan sehari-hari. perkembangan tersebut juga tidak terlepas dari munculnya kejahatan dunia maya dikenal sebagai Kejahatan Siber muncul sebagai masalah baru seiring perkembangan teknologi dan memiliki akibat yang serius baik pada tingkat individu maupun kolektif. Penelitian ini merupakan penelitian kualitatif dengan metode atau teknik deskriptif. Hasil dari penelitian ini adalah Polri mengakui tidak mudah untuk menindak kasus pidana kejahatan siber. Penanganannya berbeda dari kasus-kasus pidana lain. Cyber crime merupakan suatu tindak kejahatan yang menjadikan internet sebagai ruang atau tempat dalam melakukan kejahatan tersebut. Adapun hal yang dilakukan aparat penegak hukum ada beberapa tindakan yang dilakukan dalam pencegahan cybercrime dengan melakukan patroli siber, edukasi siber, teguran langsung melalui medsos, penindakan langsung berupa takedown medsos, penegakan hukum. Salah satu tantangan terbesar adalah kecepatan teknologi yang melebihi perkembangan regulasi yang ada, menciptakan celah keamanan yang dapat dimanfaatkan oleh pelaku kejahatan siber. Namun, tantangan terbesar mungkin mungkin terletak pada keterbatasan tenaga ahli di bidang keamanan siber. Permintaan terhadap tenaga profesional keamanan jauh melebihi

ketersediaan yang ada, sehingga banyak organisasi yang kesulitan untuk menjaga infrastruktur mereka dariancaman digital.

Kata Kunci: Cyber crime, Pencegahan, Tantangan

PENDAHULUAN

Sepanjang 2024, Polri berhasil mengungkap 325.150 kasus di Indonesia sepanjang 2024. Angka tersebut menurun dibandingkan dengan tahun 2023. Berdasarkan laporan tindak kejahatan bahwa secara umum total kejahatan (CT) pada tahun 2024 sebanyak 325.150 perkara atau menurun 14.387 perkara (4,23%) dibandingkan tahun 2023 sebesar 339.537 perkara. Pengungkapan ini berbanding lurus dengan tingkat penyelesaian perkara (CC) tahun 2024 sebesar 244.975 perkara atau 75,34%. Angka tersebut meningkat 1,09% dibandingkan tahun 2023 sebesar 74,25%. Turunnya tingkat kriminalitas di tamah air yang menurun disebabkan oleh penanganan kasus kriminalitas yang kian efektif. Hal ini tidak lupa merupakan peran besar dari Pak Listyo Sigit yang berhasil menurunkan angka kriminalitas ketika jenis aksi kejahatan kian menantang dan sulit. Hal ini merupakan suatu apresiasi besar bagi dunia polri di Indonesia yang mana selama ini terdapat keraguan tas kinerja Polri, tapi mereka tidak banyak ngeles, membela diri, atau cari pembenaran. Polri fokus bekerja dan bisa dilihat sekarang hasilnya bagus. Sekarang polri sudah sigap dan peka dalam menindak berbagai macam bentuk kejahatan, karena secara umum aksi kejahatan bisa terjadi di mana sana dan oleh siapa saja. Hal ini terbukti dari tindakan kriminalitas tidak hanya yang dilakukan oleh oknum penjahat saja, tapi juga oleh mereka yang dianggap aman.

Salah satu kejahatan di era digital adalah kejahatan siber. Era digital yang terus berkembang pesat saat ini, yaitu berupa internet dan teknologi informasi telah menjadi bagian penting dari kehidupan sehari-hari. Namun, perkembangan tersebut juga tidak terlepas dari munculnya kejahatan dunia maya dikenal sebagai Kejahatan Siber muncul sebagai masalah baru seiring perkembangan teknologi dan memiliki akibat yang serius baik pada tingkat individu maupun kolektif. Penipuan online, pencurian identitas, serangan malware, peretasan, dan penyalahgunaan data pribadi adalah contoh kejahatan dunia maya yang dilakukan melalui jaringan komputer dan Internet. Kejahatan dunia maya menjadi semakin kompleks dan meluas, berdampak pada individu, organisasi, dan negara karena perkembangan pesat teknologi informasi dan komunikasi. Berbagai aspek kehidupan, seperti ekonomi, pendidikan, dan kesehatan, telah sangat berubah selama era digital. Kejahatan siber memiliki dampak negatif pada ekonomi, keamanan, dan privasi individu, dan dapat menyebabkan kerugian finansial besar. Mereka juga dapat merusak reputasi, menimbulkan ketidakamanan, dan menimbulkan ketakutan di masyarakat. Oleh karena itu, penanganan kejahatan siber sangat penting. (Firdaus, 2024)

Kejahatan di masa sekarang ini tidak lagi sama dengan kejahatan secara konvensional, yaitu kejahatan yang perbuatannya dilakukan secara langsung di depan manusia, akan tetapi kejahatan digital memakai teknologi yang sedang berkembang saat ini yang dapat dilakukan dimana saja menggunakan teknologi teknologi masa sekarang seperti Laptop, Komputer, Handphone, dan lain-lainnya selama terdapat akses Internet dan fasilitas gadget yang memadai, sehingga kejahatan tersebut dapat di lakukan pelaku kejahatan siber dengan mudah. Internet sendiri pada awal mula adalah suatu jaringan komunikasi digital yang sampai saat ini telah menghubungkan hampir seluruh dunia melalui jaringan, oleh karenanya terasa tidak ada jarak antara satu negara dengan negara

lainnya. (Firdaus, 2024).

METODE PENELITIAN

Penelitian ini merupakan penelitian kualitatif dengan metode atau teknik deskriptif. Penelitian deskriptif adalah penelitian yang bertujuan untuk menjelaskan fenomena atau keadaan saat ini tanpa mempengaruhi atau mengubah variabel yang diamati. Data deskriptif dibuat untuk memberikan gambaran yang jelas tentang kondisi yang diteliti (Achjar, et al., 2024). Data dalam penelitian ini dikumpulkan melalui wawancara serta studi literatur yang berasal dari jurnal ilmiah maupun buku yang berkaitan dengan kejahatan siber.

HASIL DAN PEMBAHASAN

1. Kejahatan Cyber

Salah satu tindakan kejahatan yang perlu diberantas adalah kejahatan cyber. Kejahatan siber didalamnya mencakup seperti judi online dan penipuan online. Hal ini terbukti dari judi online hingga penipuan online merupakan kejahatan siber terbanyak di Tanah Air. Hal itu ia katakan saat jadi keynote speech pada Program Mentoring Berbasis Resiko (Promensisko) Tindak Pidana Pencucian Uang (TPPU) dan Pendanaan Terorisme (TPPT) dari kejahatan siber. Tindak pidana kejahatan siber naik signifikan pada 2022 bila dibandingkan dengan periode yang sama di 2021. Bahkan jumlah tindak kejahatan siber meningkat hingga 14 kali. Data di e-MP Robinopsnal Bareskrim Polri menunjukkan kepolisian menindak 8.831 kasus kejahatan siber sejak 1 Januari hingga 22 Desember 2022. Seluruh satuan kerja di Bareskrim Polri dan polda di Indonesia melakukan penindakan terhadap kasus tersebut. Polda Metro Jaya menjadi satuan kerja dengan jumlah penindakan paling banyak terhadap kasus kejahatan siber yaitu 3.709 perkara.

Sementara pada periode yang sama di 2021, jumlah penindakan yaitu 612 di seluruh Indonesia. Hanya 26 satuan kerja yang melakukan penindakan. Polri mengakui tidak mudah untuk menindak kasus pidana kejahatan siber. Penanganannya berbeda dari kasus- kasus pidana lain. Lantaran itu, Polri terus mengembangkan struktur untuk membentuk Direktorat Tindak Pidana Siber di tiap kepolisian daerah di Indonesia. Polri tengah engembangkan struktur untuk mengimbangi kejahatan siber di daerah. Polri mengusulkan direktorat yang menangani tindak pidana siber di tingkat Polda. Usulan itu diharapkan dapat meningkatkan kualitas penyidik untuk menghadapi kejahatan siber yang merambah ke daerah. Sebab penindakannya masih berstatus subdirektorat kecil di bawah tindak pidana khusus. Berdasarkan informasi di lapangan didapatkan bahwa Direktoral Tindak Pindana Siber (Dittipidsiber) yang bertugas melakukan penegakan hukum terhadap kejahatan siber. Direktorat menangani dua kelompok kejahatan terkait siber. Direktorat juga memiliki fasilitas berupa laboratorium digital forensik yang memenuhi standar mutu untuk mendukung penindakan dan pemberantasan terhadap kejahatan siber. Direktorat melayani pemeriksaan barang bukti digital dari berbagai satuan kerja, baik dari tingkat Mabes hingga Polsek. Direktorat juga menjalin kerja sama dengan berbagai instansi, baik dalam dan luar negeri, untuk memudahkan koordinasi dalam pengungkapan kejahatan siber yang bersifat transnasional dan terorganisasi. Sepanjang 2022, Polri menindak 8.831 kasus terkait kejahatan siber sejak 1 Januari sampai 22 Desember. Polri juga menindak 8.372 orang yang menjadi

terlapor dalam kejahatan tersebut. Sebagai informasi, sesuai dengan Undang Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik

Indonesia Pasal 15 ayat (1) huruf j, Polri berwenang menyelenggarakan Pusat Informasi Kriminal (Pusiknas). Pusiknas berada di bawah Bareskrim Polri serta berlandaskan regulasi Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 15 Tahun 2010 tentang Penyelenggaraan Pusat Informasi Kriminal Nasional di Lingkungan Kepolisian Negara Republik Indonesia. Pusiknas Bareskrim Polri memiliki sistem Piknas untuk mendukung kinerja Polri khususnya bidang pengelolaan informasi kriminal berbasis teknologi informasi dan komunikasi serta pelayanan data kriminal baik internal dan eksternal Polri dalam rangka mewujudkan Polri yang PRESISI (Prediktif, Responsibilitas, Transparansi Berkeadilan).

Cyber crime merupakan suatu tindak kejahatan yang menjadikan internet sebagai ruang atau tempat dalam melakukan kejahatan tersebut. Kejahatan-kejahatan tersebut mencakup kejahatan yang dilakukan melalui internet, keljahatan digital, dan kejahatan yang melibatkan jaringan telekomunikasi. Keljahatan yang telrmasuk kel dalam cyber crime masuk kel dalam ranah hukum pidana. Dalam Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP) berisikan ketentuan-ketentuan hukum yang berfungsi sebagai pelindung untuk masyarakat di berbagai kepentingan, salah satunya dalam ancaman kemajuan teknologi yaitu pada kejahatan siber atau cyber crime, seperti kasus-kasus pencurian data pribadi atau pembobolan saldo rekening korban. Terdapat beberapa faktor pemicu adanya kejahatan siber, yaitu sebagai berikut: (Duarif & Saleh, 2024)

a. Kemajuan teknologi

   Pelaku kejahatan siber mendapatkan begitu banyak kesempatan dalam melakukan aksi kejahatannya dikarenakan adanya kelmajuan teknologi, dengan memanfaatkan eksistelnsi dari perangkat-perangkat yang terhubung ke internet, serta pelaku memiliki begitu banyak cara untuk mencuri data, merusak sistem, atau lainnya dengan adanya pemanfaatan teknologi informasi yang begitu banyak.

b. Keuntungan finansial

   Terdapat dorongan finansial yang begitu besar bagi pelaku kejahatan siber dalam melakukan aksinya. Kegiatan seperti phising akan membuahkan suatu keuntungan finansial dengan jumlah yang belsar bagi pelaku.

c. Anonimitas

   Terdapat satu alasan mengapa pelaku melakukan kejahatan siber yaitu dikarenakan adanya kemampuan dari pelaku untuk melakukan aksi keljahatannya selcara anonim dengan melnggunakan jaringan privat virtual atau yang biasa dikelnal dengan VPN, atau dengan cara lainnya untuk menyembunyikan jejak mereka.

d. Kurangnya keamanan sistem

   Masih kurang memadainya keamanan suatu sistem yang menyebabkan suatu kerentanan pada perangkat lunak atau pembaruan pada sistem sehingga dapat menjadi celah bagi para pelaku untuk melakukan perubahan dalam bentuk "pengrusakkan" pada sistem yang ia serang.

e. Faktor dari manusia itu sendiri

Pelaku kejahatan siber memanfaatkan rendahnya pengetahuan pengguna dalam memanfaatkan teknologi untuk dapat melakukan aksi kejahatan sibernya seperti phising.Beberapa faktor penyebab terjadinya kejahatan siber, seperti adanya keterikatan (commitment), keterlibatan (attachmelnt), keyakinan (belief), dan keterampilan (invovement), dengan penjelasan sebagai berikut: (Duarif & Saleh, 2024)

a. Keterikatan (commitment)

Seseorang yang memiliki keterikatan pada sub sistem yang umum seperti yang terdapat di dalam organisasi, pekerjaan, sekolah, dan lainnya yang memiliki output dalam bentuk manfaat bagi banyak orang, seperti berupa benda, harta, reputasi, masa depan, dan lain sebagainya. Dengan adanya hasil dari keterikatan tersebut, seseorang akan terdorong untuk taat pada aturan yang berlaku.

b. Keterlibatan (attachment)

Keterlibatan adalah cara dari manusia untuk melibatkan dirinya sendiri terhadap orang lain, atau yang biasa kita lihat dalam kegiatan bersosialisasi atau tolong menolong antar manusia dalam pelaksanaannya, manusia melibatkan pikiran, perasaan, dan kehendak orang lain, sehingga dirinya menjadi lebih peka. Hubungan antara penyimpangan dengan "keterlibatan" yaitu sejauh apa seseorang tersebut dapat peka terhadap pikiran, perasaan, dan kehendak orang lain.

c. Keyakinan (belief)

Keyakinan dalam hal ini merupakan keyakinan atau seseorang terhadap nilai-nilai moral yang berlaku di lingkungannya yang akan menimbulkan ketaatan terhadap suatu norma.

d. Ketrampilan (invovement)

Jika seseorang aktif pada kegiatan-kegiatan positif di dalam suatu organisasi maka kecil kemungkinannya seseorang tersebut untuk melakukan penyimpangan atau deviasi.

2. Pencegahan Tindak Pidana Siber

Cybercrime merupakan salah satu kejahatan serius meskipun kelihatan tidak tampak tetapi kerugian materil maupun moril sangat bisa dirasakan oleh para korban. Ini merupakan salah satu kejahatan yang memungkinkan dilakukan oleh orang yang berada di luar yudiksi hukum atau bisa dilakukan lintas negara. Kejahatan dalam dunia maya atau cybercrime terjadi begitu banyak belakangan ini disertai dengan berbagai dinamika persoalan yang terjadi dan juga sulit untuk diatasi ataupun diselesaikan secara tindak pidana. Tindakan preventif dalam kejahatan merupakan tindakan yang mengharapkan sesuatu itu dapat ditanggulang dan dicegah sebelum kejahatan itu terjadi dalam hal yang lain menharapkan terjadinya penurunan dari kejahatan tersebut atau kejahatan tersebut dapat dihilangkan. Tujuan dari tindakan prevetif seperti pencegahan ini tidak lain tidak bukan seperti yang tertulis dalam Tugas dan wewenang Polri terulis di dalam Undang- Undang Nomor 2 Tahun 2002 tentang Kepolisian Republik Indonesia. (Agung, Hafrida, & Erwin, 2022)

Adapun hal yang dilakukan aparat penegak hukum ada beberapa tindakan yang dilakukan dalam pencegahan cybercrime dengan melakukan:

a. Patroli siber

Patroli siber adalah patroli yang dilakukan di dalam kepolisian dalam pelaksanaannya patroli siber bertujuaan untuk mengawasi segala macam bentuk pelanggaran terhadap hukum di dalam internet terkhusus aplikasi media sosial, patroli siber sendiri biasanya dilakukan pada aplikasi seperti instagram, whatsapp, twitter. Patroli siber dilakukan untuk menciptakan ruang internet yang aman serta melindungi masyarakat dari kejahatan

b. Edukasi siber

Edukasi siber sendiri pada dasarnya adalah sebuah pengenalaan al-cybercrime dan bahayanya. Edukasi siber lebih lagi ditujukan untuk memberil manfaat informasi tentang cybercrime keseluruhan baik, bahayanya, jenis-jenisnya, modusnya serta hukuman akan kejahatan tersebut.

c. Teguran langsung melalui medsos

Teguran langsung merupakan bentuk lanjutan dari patroli siber teguran langsung diharapkan untuk membuat peringatan akan pelanggaran yang dilakukan oleh masyarakat pada media sosial ataupun internet. Teguran langsung yang Polda Jambi sendiri bekerja sama dengan Kemenkominfo untuk melakukan tindakan pencegahan hal-hal yang mendapat teguran berupak konten yang bersifat provokasi, sara, ataupun pornografi.

d. Penindakan lansung berupa take down medsos

Take down merupakan salah satu strategi dari lima bentuk pencegahan yang dilakukan oleh Polda Jambi dalam mencegah cybercrime, take down sendiri jika dijelaskan adalah suatu tindakan untuk menghentikan ataupun menghapus ketersediaan sesuatu yang berada dalam ruang internet seperti video, website, berita ataupun aplikasi yang kurang baik, seperti melanggar etika, moral dan kesopanan serta hukum.

e. Penegakan hukum

Penegakan hukum merupakan salah satu bentuk pencegahan, tindakan represif sendiri diperlukan untuk memberi efek jera. Tindakan refresif merupakan upaya penanggulangan dengan menggunakan sarana penal, yang dilakukan melalui proses hukum sebagaimana yang diatur dalam ketentuan peraturan perundang-undangan terkait seperti UU ITE, KUHP, UU Pornografi dan sebagainya. Sebagaimana diuraikan pada bagian terdahulu kejahatan siber sampai saat ini yang terbanyak merupakan tindak pidana siber yang berkenaan dengan perbuatan-perbuatan lama yang telah diatur dalam peraturan lainnya tetapi dalam pelaksanaan perbuatannya menggunakan sarana komputer, internet maupun teknologi informasi lainnya. Sehingga dalam upaya penanggulangan refresif ini selalin menggunakan sarana hukum pidana UU ITE tetapi juga tidak terlepas dari peenggunaan peraturan perundang-undangan lainnya.

Penggunaan teknologi digital telah menciptakan tantangan baru dalam penegakan hukum. Misalnya, sulit untuk mengidentifikasi dan melacak pelaku kejahatan siber yang seringkali beroperasi di berbagai negara. Hukum harus mampu menyesuaikan diri dengan

kemampuan teknologi untuk menjaga penegakan hukum yang efektif. Berikut adalah beberapa hal penting dalam adaptasi hukum terhadap kemajuan teknologi dalam ranah cyber: (Purba, Maharani, BMY, & Al Zahra, 2024)

a. Penyusunan dan Pembaruan Hukum: Hukum harus terus disesuaikan dengan perkembangan teknologi dalam dunia cyber. Hal ini meliputi pembuatan undang- undang baru yang mengatur kejahatan cyber serta pembaruan terhadap undang- undang yang sudah ada agar tetap relevan dengan perkembangan teknologi.

b. Kerjasama Internasional: Kejahatan siber seringkali melintasi batas negara, sehingga kerjasama internasional dalam penegakan hukum menjadi sangat penting. Kesepakatan bilateral dan multilateral serta pertukaran informasi antar negara menjadi kunci dalam menangani kejahatan cyber yang melibatkan pelaku dari berbagai negara.

c. Pelatihan dan Peningkatan Kapasitas: Aparat penegak hukum harus diberikan pelatihan yang memadai untuk memahami teknologi yang berkembang pesat serta metode-metode yang digunakan oleh pelaku kejahatan siber. Peningkatan kapasitas ini termasuk dalam hal identifikasi, investigasi, dan penanganan kasus kejahatan siber.

d. Pengaturan Perlindungan Data: Dengan semakin banyaknya data yang disimpan dan diproses secara digital, perlindungan data menjadi kunci dalam upaya memerangi kejahatan cyber. Hukum harus memperhatikan regulasi yang mengatur penggunaan dan perlindungan data pribadi serta tindakan yang diperlukan jika terjadi pelanggaran data.

e. Ketegasan dalam Penegakan: Hukum harus menunjukkan ketegasan dalam penegakan terhadap pelaku kejahatan siber. Hukuman yang sesuai harus diterapkan untuk menimbulkan efek jera dan mencegah terulangnya tindakan kejahatan tersebut.

f. Kolaborasi dengan Industri Teknologi: Kerjasama antara pihak penegak hukum dan perusahaan teknologi menjadi penting dalam mendeteksi, mencegah, dan menangani kejahatan cyber. Keterlibatan industri teknologi dalam penyusunan kebijakan dan berbagi informasi tentang ancaman keamanan juga dapat membantu meningkatkan respons terhadap kejahatan siber.

3. Tantangan dalam Penegakan Siber

Salah satu tantangan terbesar adalah kecepatan teknologi yang melebihi perkembangan regulasi yang ada, menciptakan celah keamanan yang dapat dimanfaatkan oleh pelaku kejahatan siber. Teknologi baru, seperti kecerdasan buatan dan Internet of Things (IoT), sering kali diadopsi tanpa pertimbangan keamanan yang matang, sehingga meningkatkan risiko. Selain itu, banyak masyarakat yang masih kurang sadar akan pentingnya menjaga keamanan data mereka. Kebiasaan menggunakan kata sandi yang lemah atau mudah ditebak, serta tidak mengenali ancaman phishing, menjadi salah satu penyebab utama tingginya insiden cybercrime. Solusi atau pemecahan untuk mengatasi masalah cybercrime tidak hanya bergantung pada teknologi, tetapi juga memerlukan upaya untuk meningkatkan kesadaran publik. Edukasi melalui kampanye dan pelatihan menjadi penting untuk memperkenalkan konsep dasar keamanan digital kepada masyarakat luas. Selain itu, kerja sama internasional yang sangat diperlukan untuk menghadapi tantangan ini, mengingat sifat cybercrime yang sering kali lintas batas negara. Kerja sama antarnegara dalam rangka untuk menyusun regulasi

global yang seragam dan efisien akan mempermudah penegakan hukum dalam kasus cybercrime lintas yurisdiksi. Di sisi lain, pengembangan teknologi seperti enkripsi data dan sistem deteksi intrusi secara real-time dapat membantu mencegah serangan siber sebelum terjadi kerugian yang lebih besar. (Valentine, Septiani, & Parshusip, 2024)

Namun, tantangan terbesar mungkin mungkin terletak pada keterbatasan tenaga ahli di bidang keamanan siber. Permintaan terhadap tenaga profesional keamanan jauh melebihi ketersediaan yang ada, sehingga banyak organisasi yang kesulitan untuk menjaga infrastruktur mereka dariancaman digital. Oleh karena itu, penting bagi pemerintah dan institusi pendidikan untuk berinvestasi dalam pengembangan kurikulum yang mendukung peningkatan kompetensi di bidang keamanan siber. Secara keseluruhan, pendekatan yang holistik, mencakup peningkatan teknologi, regulasi hukum yang ketat, edukasi publik, serta kerja sama global, merupakan kunci dalam menangani ancaman cybercrime yang terus berkembang.

Dampak sosial dari cybercrime sangat luas dan dapat merusak kepercayaan publik terhadap sistem digital yang menjadi bagian penting dari kehidupan sehari-hari. Kasus- kasus pelanggaran data besar-besaran, seperti kebocoran informasi pribadi atau data perusahaan, dapat menimbulkan kerugian finansial yang signifikan dan dampak jangka panjang terhadap reputasi organisasi serta kesejahteraan individu. Perubahan dalam perilaku manusia yang dipengaruhi oleh teknologi digital, seperti kecenderungan untuk berbagi informasi pribadi secara berlebihan di media sosial, juga meningkatkan kerentanan terhadap serangan siber. Tantangan dalam Penanganan Cybercrime: (Malian, 2024)

a. Anonimitas dan Yurisdiksi

   Anonimitas: Penjahat dunia maya sering kali menggunakan metode canggih untuk menyembunyikan identitas mereka, seperti enkripsi dan web gelap. Dalam masalah yurisdiksi, Cybercrime sering kali melintasi batas negara, mempersulit proses hukum dan koordinasi antara berbagai negara.

b. Kemajuan Teknologi yang Pesat

   Teknologi berkembang lebih cepat daripada kemampuan lembaga penegak hukum untuk beradaptasi, sehingga sulit untuk mengikuti jenis Cybercrime dan taktik baru.

c. Kompleksitas Cybercrime

   Cybercrime mencakup peretasan, phishing, ransomware, pencurian identitas, dan banyak lagi, yang masing-masing memerlukan pendekatan berbeda. Investigasi yang efektif sering kali menuntut pengetahuan yang sangat terspesialisasi dalam teknologi informasi dan keamanan siber.

d. Pengumpulan dan Pelestarian Bukti

   Bukti digital dapat bersifat tidak stabil dan mudah diubah atau dihancurkan. Memastikan integritas bukti digital merupakan tantangan yang signifikan.

e. Keterbatasan Sumber Daya

   Banyak lembaga penegak hukum tidak memiliki sumber daya yang diperlukan, termasuk personel dengan keterampilan khusus dan teknologi canggih, untuk memerangi kejahatan

siber secara efektif.

f. Masalah Privasi

Menyeimbangkan pemberantasan kejahatan yang efektif dengan menghormati privasi dan kebebasan sipil dapat menjadi tantangan, terutama jika pengawasan dan pengumpulan data terlibat.

Penegakan hukum siber di Indonesia menghadapi berbagai tantangan signifikan yang mempengaruhi efektivitasnya: (Sitanggang, Darmawan, & Manurung, 2024)

a. Kurangnya Sumber Daya: Banyak instansi penegak hukum kekurangan perangkat dan teknologi canggih untuk mendeteksi dan melacak aktivitas siber yang ilegal.

b. Keterampilan Teknis: Ada kebutuhan mendesak untuk pelatihan dan pengembangan keterampilan bagi penegak hukum untuk memahami dan menangani kejahatan siber secara efektif.

c. Koordinasi Antar Lembaga: Kurangnya koordinasi antara berbagai lembaga terkait menyebabkan penanganan kasus kejahatan siber seringkali tidak efisien.

d. Hukum Internasional: Kejahatan siber seringkalı melibatkan pelaku lintas negara, sehingga memerlukan kerjasama internasional yang kuat untuk penegakan hukum.

Untuk mengatasi tantangan yang dihadapi dalam penegakan hukum siber di Indonesia, beberapa solusi dapat diimplementasikan: (Sitanggang, Darmawan, & Manurung, 2024)

a. Peningkatan Kapasitas Teknologi: Investasi dalam teknologi canggih untuk mendeteksi dan melacak aktivitas siber yang mencurigakan sangat diperlukan. Ini termasuk pengembangan alat forensik baru dan sistem monitoring yang lebih canggih.

b. Pelatihan dan Pendidikan: Program pelatihan berkelanjutan bagi penegak hukum untuk meningkatkan keterampilan teknis dalam menangani kejahatan siber. Ini mencakup kursus dalam analisis forensik digital, keamanan jaringan, dan hukum siber.

c. Kerjasama Antar Lembaga: Membangun sistem koordinasi yang lebih baik antara berbagai lembaga penegak hukum dan institusi terkait. Ini dapat dilakukan melalui pembentukan tim tanggap darurat siber yang terkoordinasi dengan baik.

d. Kerjasama Internasional: Mengembangkan kerjasama internasional yang lebih kuat melalui perjanjian bilateral dan multilateral untuk menghadapi kejahatan siber yang bersifat lintas negara. Ini mencakup. pertukaran informasi, pelatihan bersama, dan operasi penegakan hukum bersama.

KESIMPULAN

1. Polri mengakui tidak mudah untuk menindak kasus pidana kejahatan siber. Penanganannya berbeda dari kasus-kasus pidana lain. Cyber crime merupakan suatu tindak kejahatan yang menjadikan internet sebagai ruang atau tempat dalam melakukan kejahatan tersebut.
2. Adapun hal yang dilakukan aparat penegak hukum ada beberapa tindakan yang dilakukan dalam pencegahan cybercrime dengan melakukan patroli siber, edukasi siber, teguran langsung melalui medsos, penindakan langsung berupa takedown medsos, penegakan hukum.

3. Salah satu tantangan terbesar adalah kecepatan teknologi yang melebihi perkembangan regulasi yang ada, menciptakan celah keamanan yang dapat dimanfaatkan oleh pelaku kejahatan siber. Namun, tantangan terbesar mungkin mungkin terletak pada keterbatasan tenaga ahli di bidang keamanan siber. Permintaan terhadap tenaga profesional keamanan jauh melebihi ketersediaan yang ada, sehingga banyak organisasi yang kesulitan untuk menjaga infrastruktur mereka dariancaman digital.

DAFTAR PUSTAKA

Achjar, K., Primasari, D., Putra, R., Sartono, S., Rays, I., Febriani, A., . . . Prastyadewi, M. (2024). *Buku Ajar Metodologi Penulisan Karya Ilmiah.* Jambi: Sonpedia Publishing Indonesia.

Agung, A., Hafrida, & Erwin. (2022). Pencegahan Kejahatan Terhadap Cybercrime. *PAMPAS: Journal of Criminal, 3*(2), 212-222.

Duarif, & Saleh, M. (2024). Pencegahan dan Penindakan Tindak Pidana Siber Oleh Kepolisian Resort Teluk Bintuni. *UNES LAW REVIEW, 6*(4), 12110-12119.

Firdaus, R. (2024). Perlindungan Hukum dan Pencegahan Kejahatan SIber di Era Digital dalam Sistem Hukum di Indonesia. *STAATSRECHT: Jurnal Hukum Kenegaraan dan Politik Islam, 4*(1), 79-104.

Malian, D. (2024). Penanganan dan TAntangan Cybercrime di Era Digital Perspektif Kriminologi. *INNOVATIVE: Journal of Social Science Research, 4*(6), 7084-7056.

Purba, R., Maharani, D., BMY, M., & Al Zahra, R. (2024). Peranan Hukum Positif dalam Mengatur Cyberspace untuk Menghadapi Tantangan dan Peluang di Era Digital. *MANDUB: Jurnal Politik, Sosial, Hukum dan Humaniora, 2*(2), 167-176.

Sitanggang, A., Darmawan, F., & Manurung, D. (2024). Hukum Siber dan Penegakan Hukum di Indonesia: Tantangan dan Solusi dalam Memerangi KEjahatan SIber. *Jurnal Pendidikan dan Teknologi Indonesia (JPTI), 4*(3), 79-83.

Valentine, V., Septiani, C., & Parshusip, J. (2024). Menghadapi Tantangan dan Solusi Cybercrime di Era Digital. *Informatech: Jurnal Ilmiah Informatika dan Komputer, 1*(2), 152-156.