Hukum Internasional dan Tantangan Cybersecurity: Keamanan Digital di Era Global

Sechilia Herdianti Nur[1], Padrisan Jamba[2]
[1]Ilmu Hukum, Ilmu Sosial dan Humaniora, Universitas putera Batam
[2]Ilmu Hukum, Ilmu Sosial dan Humaniora, Universitas putera Batam

*Pb230710007@upbatam.ac.id
*Padrisan@puterabatam.ac.id

ABSTRAK

Hukum internasional mempunyai peran penting dalam mengatasi tantangan keamanan *Cyber* di era digital yang saling terhubung. Keamanan *cyber* ini mencakup pada perlindungan data dan infrastruktur digital yang menjadi krusial. Maka menjalun kerjasama internasional, regulasi yang efektif serta peningkatan kesadaran menjadi kunci utama dalam menghadapi *cyber* yang kompleks dan terus berkembang. Perkembangan teknologi informasi dan komunikasi di era digital ini juga telah memberikan manfaat yang besar, namun juga menghadirkan tantangan serius dalam bentuk ancaman *cyber*.

Kata Kunci : Serangan *cyber* internasional, Hukum Internasional, Keamanan *cyber*

ABSTRACT

International law have an important role in addressing cyber security challenges in the interconnected digital era. Cyber security includes data protection and digital infrastructure that are crucial. Therefore, establishing international cooperation, effective regulation and increasing awareness are the main keys in dealing with complex and ever-evolving cyber. The development of information and communication technology in this digital era has also provided great benefits, but also presents serious challenges in the form of cyber threats.

Keyword : International *Cyber Attack, International Law, Cyber Security*

1. PENDAHULUAN

Pada era yang semakin pesat perkembangannya seperti saat ini, cyber space atau ruang cyber telah menjadi sebuah kebutuhan dasar yang memungkinkan manusia untuk terhubung tanpa batas fisik. Keamanan cyber menjadi suatu hal yang sangat penting mengingat bahwa meningkatnya frekuensi dan skala serangan cyber yang dapat menyebabkan seseorang mengalami kerugian secara finansial, kehilangan data pribadi, serta ancaman terhadap keamanan nasional terhadap suatu negara.

Oleh karena itu, kebutuhan akan peraturan dan regulasi yang menyeluruh dan efektif menjadi sangat mendesak untuk melindungi data dan sistem informasi dari berbagai ancaman *cyber*. Dalam upaya mengatasi ancaman *cyber*, berbagai peraturan telah diterapkan oleh pemerintah diseluruh dunia. Peraturan tersebut bertujuan untuk melindungi data pribadi seseorang, memastikan integritas sistem informasi, dan menegakkan hukum terhadap pelaku kejahatan *cyber*. Regulasi keaman cyber juga menjadi pendorong dalam penerapan pratik terbaik dalam manajemen risiko dan meningkatkan kesadaran tentang pentingnya keamanan informasi. Negara negara diseluruh dunia saat ini telah menyadari pentingnya mengembangkan aturan hukum yang kuat dalam menghadapi tantangan ini. (Maesaroh, 2024)

Berbagai cara atau strategi telah diterapkan, mulai dari undang- undang nasional, standar industri, sampai dengan kebijakan pemerintah yang bertujuan untuk memperkuat keamanan cyber. Namun, keberhasilan dari upaya ini sangat bergantung pada kerjasama internasional, mengingat sifat ancaman cyber yang tidak mengenal batas geografis artinya serangan cyber bisa terjadi dimana saja dan terhadap siapa saja.(Maesaroh, 2024)

Berkembangnya salah satu teknologi yang sering digunakan seperti internet telah memunculkan bentuk kejahatan baru yang dikenal sebagai cybercrime atau kejahatan yang dilakukan melalui jaringan internet. Beberapa contoh kasus cybercrime di Indonesia yaitu pencurian data kartu kredit, peretasan (hacking) situs web, penyadapan data seperti email, serta manipulasi data dengan menyisipkan instruksi yang tidak diinginkan ke dalam program komputer. Dalam kejahatan berbasis komputer, dikenal dua jenis delik, yaitu delik formil dan delik materil. Delik formil terjadi ketika seseorang mengakses komputer orang lain tanpa izin, sedangkan delik materil adalah tindakan yang menyebabkan kerugian bagi pihak lain. Kejahatan cybercrime ini menjadi ancaman serius terhadap stabilitas, sementara pemerintah menghadapi tantangan dalam mengimbangi teknik-teknik kejahatan yang semakin canggih dengan pemanfaatan teknologi komputer, khususnya yang melibatkan jaringan internet dan internet.

2. METODE PELAKSANAAN

Penelitian ini menggunakan metode penelitian kualitatif sebagai sumbermetode utamanya. Pengumpulan data dikumpulkan

melalui studi literatur yang bersumber dari buku dan jurnal penelitian ilmiah mengenai topik terkait kemudian untuk menganalisanya menggunakan teori/perspektif. Dengan demikian data yang berhasil dikumpulkan dapat dipahami secara lengkap dan menyeluruh. Tujuan Utama penelitian ini adalah untuk memahami dan menjelaskan mengenai Hukum Internasional dan Tantangan Cybersecurity : Keamanan Digital di Era Global.

Selain itu metode ini berusaha mengumpulkan, menyusun dan menginterpretasikan data yang kemudian akan diajukan dengan menganalisis suatu fenomena serta suatu metode dalam meneliti status kelompok manusia, suatu objek, dan suatu kelas peristiwa pada masa sekarang. referensi jurnal yang berhubungan dengan masalah yang sedang diteliti dengan tujuan untuk mengumpulkan informasi yang tepat mengenai Cyber Security.

3. HASIL DAN PEMBAHASAN

Kejahatan cyber telah menjadi ancaman serius di era digital saat ini. Sifatnya yang lintas batas dan sangat cepat berkembang membuat penegakan hukum di setiap negara menghadapi berbagai tantangan, terutama dalam hal pembuktian. Artikel ini akan membahas beberapa tantangan utama di dalam pembuktian kasus kejahatan cyber serta upaya yang dapat dilakukan untuk mengatasinya :

A. Volatilitas Bukti Digital

Bukti digital bersifat mudah berubah atau hilang. Data dapat dengan cepat dihapus, dimodifikasi, atau rusak, baik secara sengaja maupun tidak sengaja . Hal ini membuat proses pengumpulan dan preservasi bukti digital menjadi sangat krusial dan menantang. Untuk mengatasi masalah ini, para penegak hukum perlu mengembangkan prosedur forensik digital yang ketat dan standar. Penggunaan teknik imaging forensik dan hash values dapat membantu menjaga keaslian bukti digital.

B. Sifat transnasional kejahatan cyber (kejahatan melibatkan lebih dari satu negara)

satu tantangan terbesar dalam pembuktian kasus kejahatan cyber adalah sifatnya yang transnasional. Pelaku dapat melakukan kejahatan dari satu negara, sementara korban berada di negara lain dan bukti digital tersebar di berbagai yurisdiksi Hal ini menyulitkan proses pengumpulan bukti dan penegakan hukum. Untuk mengatasi tantangan ini, diperlukan kerjasama internasional yang lebih kuat dalam penanganan kejahatan cyber. Konvensi Budapest tentang Kejahatan cybertahun 2001 telah menjadi langkah awal yang baik, namun masih perlu ditingkatkan penerapannya. Perjanjian ekstradisi dan bantuan hukum timbal balik (MLA) antar negara juga perlu diperkuat untuk memfasilitasi pertukaran informasi dan bukti digital lintas batas.

C. Enkripsi dan Anonimitas (tidak diketahui)

Teknologi enkripsi dan tools anonimitas seperti VPN atau Tor memungkinkan pelaku kejahatan cyber untuk menyembunyikan identitas dan aktivitas mereka Hal ini membuat proses pelacakan dan pembuktian menjadi lebih sulit. Untuk menghadapi tantangan ini, penegak hukum perlu mengembangkan kemampuan dalam teknik dekripsi dan analisis lalu lintas jaringan. Kerjasama dengan penyedia layanan internet dan

platform teknologi juga penting untuk memperoleh informasi yang diperlukan. Namun, upaya ini harus tetap memperhatikan keseimbangan antara penegakan hukum dan perlindungan privasi pengguna internet yang sah.

D. Cepat berkembangnya Teknologi

Teknologi yang digunakan dalam kejahatan cyber berkembang sangat cepat, sering kali lebih cepat daripada kemampuan penegak hukum untuk mengikutinya Hal ini menciptakan tantangan konstan dalam pemahaman dan pengumpulan bukti yang bersangkutan dengan kejahatan yang melibatkan teknologi baru. Untuk mengatasi tantangan ini, lembaga penegak hukum perlu terus memperbarui pengetahuan dan keterampilan mereka. Kerjasama dengan sektor swasta dan akademisi dalam penelitian dan pengembangan forensik digital juga sangat penting . Selain itu, pembentukan unit khusus kejahatan cyber dengan keahlian teknis yang mendalam dapat membantu meningkatkan kapasitas penanganan kasus kasus kompleks. (Qalbi et al., 2020)

CONTOH KASUS CYBER CRIME DI DUNIA

Kasus pembobolan pada beberapa lembaga perbankan di Amerika yang dilakukan oleh 5 warga negara Rusia, Kelima pelaku tersebut bekerja sama memasuki sistem keamanan lembaga keamanan dengan cara menonaktifkan peranngkat lunak anti-virus lembaga perbankan dan pengumpulan data hasil pencurian pada beberapa platform milik mereka, kemudian mendistribusikan dan menjualnya. Data hasil pencurian tersebut berupa nomor dari kartu kredit dan kartu debet milik lembaga perbankan. Penanganan terhadap kasus tersebut mengalami kesulitan terutama dikarenakan para pelaku hacking tersebut berwarganegara Rusia karena Rusia tidak pernah ingin mengekstradisikan. (Setialana, 2014)

Tantangan dalam pembuktian kasus kejahatan cyber memang kompleks dan multifaset. Namun, dengan pendekatan yang komprehensif meliputi peningkatan kerjasama internasional, pengembangan kapasitas teknis, harmonisasi hukum dan standar, serta inovasi dalam metode investigasi,tantangan-tantangan tersebut dapat diatasi. Penting untuk terus mengembangkan strategi dan tools baru dalam menghadapi evolusi kejahatan cyber, sambil tetap menjaga keseimbangan antara penegakan hukum dan perlindungan hak-hak digital warga negara. Dengan upaya bersama dari berbagai pemangku kepentingan, termasuk pemerintah, sektor swasta, dan masyarakat sipil, diharapkan kemampuan dalam pembuktian kasus kejahatan cyber dapat terus ditingkatkan. Hal ini pada akhirnya akan berkontribusi pada penciptaan lingkungan digital yang lebih aman dan terpercaya bagi semua pengguna.

Para karakter hacker biasanya tak berasal dari kaum bawah, mereka biasanya ialah orang-orang terpelajar, yangsetidaknya mengenyam

pendidikan sampai tingkat tertentu dan bisa menggunakan ataupun mengoperasikan komputer. Para craker juga termasuk orang yang berpendidikan, tidak buta teknologi, mampu menurut finansial, serta tidak termasuk dalam masyarakat kelas bawah. Kejahatan seperti ini dapat diklasifikasikan sebagai "white collar crime" (kejahatan kerah putih). Jo Ann

L. Miller, membagi pelakunya menjadi 4 (empat) kategori:

1. Organizational occupational crime Penjahat melakukan tindakan ilegal atau merugikan orang lain lewat jaringan internet buat kepentingan atau keuntungan suatu perusahaan. Pelaku biasanya adalah para eksekutif.
2. Government occupational crime Melakukan suatu tindakan yang ilegal melalui internet, namun dengan persetujuan atau perintah darinegara (pemerintah), Pelakunya sendiri ialah pejabat (birokrat) meski dalam banyak kasus bilamana hal tersebut terkuak, maka akan dibantah.
3. Professional occupational crime Beragam pekerjaan yang melakukan kejahatan secara disengaja (malpraktik).
4. Individual occupational crime Ialah para pengusaha, pemilik modal atau orang-orang independen lainnya yang melakukan perbuatan menyimpang, walaupun tingkat sosial ekonominya mungkin tidak tinggi. Dalam aspek pekerjaannya.

PENANGGULANGAN CYBER CRIME

Tindak pidana cybercrime memakan korban dengan jumlah sangat besar, terutama dari segi finansial. Kebanyakan dari korban hanya bisa menyesali apa yang sudah terjadi. Mereka berharap bisa belajar banyak dari pengalaman mereka saat ini, dan yang perlu dilakukan sekarang adalah mencegah kemungkinan- kemungkinan yang dapat merugikan kita sebagai pelaku IT. Pencegahan tersebut dapat berupa :

1. Educate user (memberikan pengetahuan baru tentang Cyber Crime dan dunia internet)
2. Use hacker's perspective (menggunakan pemikiran hacker untuk melindungi sistem anda)
3. Patch system (menutup lubang- lubang kelemahan pada sistem)
4. Policy (menetapkan kebijakan dan aturan untuk melindungi sistem Anda dari orang-orang yang tidak berwenang)
5. IDS (Intrusion Detection System) bundled with IPS (Intrusion Prevention System)
6. Firewall.
7. AntiVirus.

4. KESIMPULAN

Cyber crime telah menjadi ancaman global yang serius di era digital, dengan tantangan utama yang bersifat lintas batas, cepat berkembang, dan sulit dibuktikan secara hukum. Hukum internasional memainkan peran penting dalam menghadapi tantangan ini melalui kerangka kerja hukum yang kuat, harmonisasi regulasi antarnegara, serta kerja sama internasional. Tantangan teknis seperti volatilitas bukti digital, enkripsi, dan anonimitas memperumit proses dan penegakan hukum. Oleh karena itu, dibutuhkan peningkatan kapasitas teknis aparat penegak hukum, penguatan kerjasama lintas negara, serta keterlibatan sektor swasta dan akademisi dalam riset dan pengembangan forensik digital. Kasus besar seperti pembobolan bank menunjukkan bahwa kejahatan cyber dapat berdampak luas pada kepercayaan publik dan stabilitas ekonomi. Strategi pencegahan seperti edukasi pengguna, peningkatan sistem keamanan, serta penggunaan teknologi pertahanan cyber seperti firewall, IDS/IPS, dan antivirus, juga penting untuk menciptakan.

DAFTAR PUSTAKA

Maesaroh, R. S. (2024). *Tantangan Keamanan Siber dan Implikasinya terhadap Hukum Kenegaraan : Tinjauan atas Peran Negara dalam Menjamin Ketahanan Digital*. *4*(2).

Qalbi, N. S., Marinda, F., & Yulianti, R. (2020). Asean Against siber Terorrism: Upaya Mengatasi Propaganda Hitam Sebagai Kejahatan Siber Terorganisir. *LEGISLATIF (Lembaran Gagasan Mahasiswa Yang Solutif Dan Inovatif)*, *4*(1), 113–114.

Setialana, P. (2014). No Title ن. *Pontificia Universidad Catolica Del Peru*, *8*(33), 44.

Berlian, C. (2020). *Cheny Berlian Universitas Muhammadiyah Riau , Indonesia , chenyberlian@umri.ac.id Abstract Keywords : Cyber Crime , UU ITE Abstrak Kata kunci : Kejahatan Siber , UU ITE dampak yang cukup luas bagi hampir*

PENDAHULUAN Kemunculan teknologi digital dalam duni.

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2), 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426

Hamdan Mustameer. (2022). Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0. *Jurnal Yustika: Media Hukum Dan Keadilan*, *25*(01), 40–53. https://doi.org/10.24123/yustika.v25i01.5090

Ketaren, E. (2017). Cybercrime, Cyber Space, Dan Cyber Law. *Jurnal TIMES*, *5*(2), 35–42. https://doi.org/10.51351/jtm.5.2.2016556

Maskun, Manuputty, A., Noor, S. M., & Sumardi, J. (2013). Kedudukan Hukum Cyber Crime Dalam Perkembangan Hukum Internasional Kontemporer. *Masalah-Masalah Hukum*, *42*(4), 511–519.