Volume 14 No 1 (2026)
E- ISSN : 2580-2461
P-ISSN: 2339-1693
https://ejournal.upbatam.ac.id/index.php/cahayakeadilan

JURNAL CAHAYA KEADILAN

RANSOMEWARE GLOBAL DAN KEJAHATAN SIBER: STUDI KASUS WANNACRY DALAM PERSPEKTIF HUKUM INTERNASIONAL

Almira Fatiah Bella[1], Padrisan Jamba[2]
[1,2]Jurusan Ilmu Hukum, Fakultas Ilmu Sosial danHumaniora, Universitas Putera Batam, Kepulauan Riau

Email Koresponden : pb230710023@upbatam.ac.id

Abstrak

Serangan ransomware WannaCry tahun 2017 menjadi peristiwa penting dalam sejarah kejahatan siber global. Serangan ini menyebar ke lebih dari 150 negara dan melumpuhkan berbagai infrastruktur kritikal.Artikel ini mengkajikasus WannaCry dari perspektif hukum internasional untukmelihat sejauh mana instrumen hukum yang ada, seperti Konvensi Budapest dan prinsip tanggung jawab negara (due diligence), dapat menangani kejahatan siber lintas negara. Pendekatan yang digunakan adalah yuridis-normatif dengan metode studi kasus. Hasil kajian menunjukkan bahwa belum ada kerangka hukum internasionalyang efektif dan mengikat dalam menghadapiancaman digitalberskala global.Kelemahan koordinasi antarnegara, masalah yurisdiksi, dan anonimitas pelaku menjadi hambatan utama. Meski demikian, serangan ini mendorong lahirnya berbagai kebijakan keamanan digital, seperti pembentukan BSSN di Indonesia, penguatan kerja sama internasional, dan adopsi model keamanan zero-trust. Diperlukan pembentukan kesepakatan hukum internasional yang lebih inklusif serta penguatan kapasitas negara berkembang dalam menghadapi kejahatan siber.

Kata Kunci; Ransomware; WannaCry; Kejahatan Siber; Hukum Internasional; Keamanan Digital.

I. Pendahuluan

I.1 Latar Belakang

Perkembangan teknologi informasi yang pesat telah membawa dampak luar biasa bagi kehidupan manusia modern. Kemajuan ini memang memberikan kemudahan dalam berbagai aspek kehidupan, seperti komunikasi, perdagangan, pelayanan publik, dan akses terhadap informasi. Namun, di balik kemudahan tersebut, terbuka pula ruang baru bagi munculnya kejahatan digital yang memiliki dimensi berbeda dibandingkan dengan kejahatan konvensional. Salah satu bentuk kejahatan siber yang paling mengkhawatirkan dewasa ini adalah serangan ransomware (Ridwan, 2020).

Ransomware merupakan jenis perangkat lunak berbahaya (malware) yang bekerja dengan cara mengenkripsi data milik korban dan kemudian menuntut pembayaran tebusan agar data tersebut dapat diakses kembali. Serangan ini tidak hanya menyasar individu, tetapi juga menyerang institusi penting

seperti rumah sakit, lembaga pemerintah, universitas, bahkan sistem transportasi nasional. Ransomware telah menjelma menjadi senjata digital yang ampuh dalam lanskap konflik dan kejahatan modern (UNODC, 2021).

Salah satu insiden ransomware paling mencolok dalam sejarah dunia terjadi pada Mei 2017, ketika varian malware bernama WannaCry menyerang sistem komputer secara masif di lebih dari 150 negara. Serangan tersebut menginfeksi lebih dari 200.000 perangkat komputer dalam waktu singkat,melumpuhkanoperasirumahsakit di Inggris (NHS), perusahaan logistik global, hingga infrastruktur publik di berbagai negara. Laporan Europol mencatat bahwa serangan WannaCry memanfaatkan kerentanan sistem operasi Windows yang sebelumnya telah diketahui dan dieksploitasi oleh kelompok peretas yang diduga memiliki afiliasi dengan aktor negara (Europol, 2017).

Serangan WannaCry menjadi simbol dari era baru perang digital—konflik yang tidak lagi menggunakan senjata konvensional,tetapi kode dan algoritma sebagai alat serangnya. Kejahatan siber ini memaksa komunitas internasional untuk mengevaluasi kembali efektivitas sistem hukum internasional yang selama ini berfokus pada yurisdiksi fisik dan batas negara. Masalah utamanya terletak pada bagaimana hukum internasional dapat menjangkau dan mengatur pelaku serangan siber lintas negara yang seringkali sulit diidentifikasi dan tidak terikat secara langsung oleh yurisdiksi negara tertentu (Schmitt, 2013).

Hukum internasional publik sebenarnya telah mengatur prinsip-prinsip dasar seperti kedaulatan negara, non-intervensi, serta tanggung jawab negara dalam tindakan yang merugikan negara lain. Namun, dalam konteks kejahatan siber seperti WannaCry, pelaku seringkali beroperasi secara anonim dan memanfaatkan infrastruktur global, sehingga menimbulkan tantangan dalam aspek atribusi dan penegakan hukum (Hathaway et al., 2012). Mekanisme kerja sama internasional seperti Budapest Convention on Cybercrime telah menjadi salah satu instrumen penting dalam memerangi kejahatan siber, tetapi belum semua negara, termasuk Tiongkok dan Rusia, menjadi pihak dalam konvensi ini (Council of Europe, 2001).

Dengan demikian, kasus WannaCry bukan hanya sekadar serangan teknologi, melainkan juga menjadi pengingat akan pentingnya pembaruan instrumen hukum internasional agar mampu menanggapi dinamika kejahatan global masa kini. Dunia membutuhkan kerangka hukum yang adaptif, kolaboratif, dan transnasional untuk menghadapi ancaman siberyang semakinkompleks danmelintasi batas-batas negara.

II. Metode Penelitian

Penulisan artikel ini menggunakan pendekatan yuridis-normatif, yaitu suatu metode penelitian hukum yang berfokus pada studi terhadap norma-norma hukum yang berlaku, baik berupa aturan tertulis

dalam peraturan perundang-undangan maupun prinsip-prinsip hukum internasional yang berkembang. Pendekatan ini digunakan untuk menganalisis bagaimana hukum internasional saat ini merespons fenomena kejahatan siber lintas negara, khususnya serangan ransomware WannaCry yang terjadi pada tahun 2017.

Pendekatan yuridis-normatif dalam artikel ini digunakan untuk menelaah:

- Instrumen hukum internasional yang relevan, seperti Convention on Cybercrime (Budapest Convention 2001),
- Ketentuan hukum internasional publik, termasuk Piagam Perserikatan Bangsa-Bangsa Pasal 2(4),
- Prinsip due diligence dalam tanggung jawab negara,
- Literasi terhadap doktrin dan pendapat para ahli hukum internasional.

Selain pendekatan normatif, penulisan ini juga menggunakan metode studi kasus terhadap seranganransomware WannaCry. Studi ini digunakan untuk menggambarkan secara konkret bagaimana bentuk dan dampak kejahatan siber berskala global, serta tantangan dalam menetapkan pertanggungjawaban pelaku yang diduga terafiliasi dengan aktor negara. Studi kasus ini juga memperkuat analisis normatif dengan fakta-fakta empirik dari insiden aktual.internasional yang berkembang. Pendekatan ini digunakan untuk menganalisis bagaimana hukum internasional saat ini merespons fenomena kejahatan siber lintas negara, khususnya serangan ransomware WannaCry yang terjadi pada tahun 2017.

Pendekatan yuridis-normatif dalam artikel ini digunakan untuk menelaah:

- Instrumen hukum internasional yang relevan, seperti Convention on Cybercrime (Budapest Convention 2001),
- Ketentuan hukum internasional publik, termasuk Piagam Perserikatan Bangsa-Bangsa Pasal 2(4),
- Prinsip due diligence dalam tanggung jawab negara,
- Literasi terhadap doktrin dan pendapat para ahli hukum internasional.

Selain pendekatan normatif, penulisan ini juga menggunakan metode studi kasus terhadap serangan ransomware WannaCry. Studi ini digunakan untuk menggambarkan secara konkret bagaimana bentuk dan dampak kejahatan siber berskala global, serta tantangan dalam menetapkan pertanggungjawaban pelaku yang diduga terafiliasi dengan aktor negara. Studi kasus ini juga memperkuat analisis normatif dengan fakta-fakta empirik dari insiden aktual.yang digunakan untuk analisis data/uji korelasi.

III. Hasil Penelitian Dan Pembahasan

Konsep Ransomware dan Karakteristik Kejahatan Siber

Ransomware merupakan salah satu jenis malware yang bekerja dengan cara mengenkripsi atau mengunci data korban, kemudian meminta tebusan—biasanya dalam bentuk mata uang kripto—untuk mengembalikan akses terhadap data tersebut. Karakteristik ransomware sangat khas: bersifat anonim, lintas batas negara, cepat menyebar, serta sangat sulit dilacak (UNODC, 2021). Laporan Interpol dan United Nations Office on Drugs and Crime (UNODC) menunjukkan bahwa sejak 2015, ransomware menjadi salah satu bentuk kejahatan digital yang berkembang paling pesat. Hal ini tidak terlepas dari mudahnya memperoleh perangkat lunak berbahaya melalui pasar gelap (dark web), serta meningkatnya penggunaan Bitcoin dan cryptocurrency lainnya yang sulit dilacak secara finansial (Interpol, 2022).

Berbeda dari kejahatan pidana konvensional yang biasanya terjadi dalam satu yurisdiksi dengan pelaku dan korban yang dapat diidentifikasi secara langsung, kejahatan siber seperti ransomware justru bersifat transnasional. Dalam banyak kasus, pelaku berasal dari satu negara, menyerang korban di negara lain, dengan menggunakan server di negara ketiga. Konfigurasi ini menciptakan ruang abu-abu dalam penegakan hukum, karena masing-masing yurisdiksi memiliki batas kewenangan berbeda (Hathaway et al., 2012). Ransomware adalah bagian dari kejahatan siber yang semakin kompleks. Ia tidak dibatasi oleh batas geografis dan sangat bergantung pada teknologi kriptografi serta ekosistem jaringan gelap. Pelaku biasanya mengeksploitasi kerentanan pada sistem operasi atau aplikasi yang belum diperbarui, lalu mengirim malware yang secara otomatis mengenkripsi seluruh data korban begitu berhasil menginfeksi sistem. Karena sifat transnasionalnya, kejahatan ini sulit dihadapi dengan pendekatan hukum domestik saja. Ketika serangan berasal dari luar negeri dan berdampak secara global, diperlukan respons hukum yang berskala internasional.

Studi Kasus Serangan WannaCry: Serangan Siber Berskala Global

Pada 12 Mei 2017, dunia dikejutkan oleh serangan ransomware berskala besar yang dikenal dengan nama WannaCry. Dalam hitungan jam, serangan ini menyebar ke lebih dari 200.000 sistem komputer di 150 negara, termasuk lembaga pemerintahan, rumah sakit, institusi pendidikan, dan perusahaan logistik (Europol, 2017).

WannaCry mengeksploitasi celah keamanan pada sistem operasi Windows yang dikenal sebagai EternalBlue. Celah ini awalnya dikembangkan oleh Badan Keamanan Nasional Amerika Serikat (NSA) sebagai alat mata-mata digital, namun bocor ke publik setelah diretas oleh kelompok bernama Shadow Brokers. Malware WannaCry memanfaatkan celah tersebut untuk menyebar secara otomatis melalui jaringan lokal dan global. Korban diminta membayar tebusan sebesar $300 dalam bentuk

Bitcoin, yang akan meningkat jika pembayaran tidak dilakukan dalam waktu 72 jam (Greenberg, 2018).

Salah satu korban terbesar adalah National Health Service (NHS) di Inggris. Layanan kesehatan ini terpaksa membatalkanoperasi, menolakpasien, dan menghentikan layanan darurat karena seluruh sistem komputer mereka terkunci. Perusahaan logistik global seperti FedEx, serta perusahaan transportasi publik seperti Deutsche Bahn di Jerman juga terdampak serius.

Banyak lembaga intelijen, termasuk NSA dan Microsoft, menunjuk kelompok Lazarus Group—yang diduga berafiliasi dengan Korea Utara—sebagai aktor di balik serangan ini. Namun hingga kini, tidak ada proses hukum internasional terbuka yang mampu membuktikan secara yuridis keterlibatan negara tersebut. Hal ini memperlihatkan kesenjangan besar antara dugaan intelijen dan pembuktian hukum dalam ranah siber (Schmitt, 2013).

Hukum Internasional dan Kejahatan Siber

Saat ini, belum ada satu pun perjanjian hukum internasional yang mengikat secara global terkait kejahatan siber. Konvensi Budapest tahun 2001 merupakan satu-satunya dokumen hukum internasional yang cukup signifikan, disusun oleh Dewan Eropa dan telah diratifikasi lebih dari 60 negara. Konvensi ini mengatur definisi tindak pidana komputer, prosedur investigasi digital, dan kerangka kerja sama antarnegara. Namun, negara besar seperti Tiongkok, Rusia, dan India menolak ratifikasi dengan alasan menjaga kedaulatan digital mereka (Council of Europe, 2001).

Hukum internasional publik, melalui prinsip due diligence, menyatakan bahwa negaraberkewajibanmencegahwilayahnya digunakan untuk menyerang negara lain. Prinsip ini sudah ditegaskan dalam berbagai putusan Mahkamah Internasional, namun masih sangat terbatas implementasinya dalam konteks siber karena tidak semua negara memiliki kemampuan teknis untuk memantau dan mencegah serangan dari wilayahnya (Tallinn Manual, 2013).

Dalam kerangka hukum tentang use of force, sebagian akademisi menyebut bahwa serangan siber dapat diklasifikasikan sebagai tindakan bersenjata jika dampaknya setara dengan serangan militer. Namun, WannaCry belum memenuhi ambang batas ini sehingga tidak dapat dikategorikan sebagai tindakan agresi menurut Pasal 2 ayat 4 Piagam PBB.

Tantangan Penegakan Hukum Siber Internasional

Beberapa tantangan utama dalam penegakan hukum siber lintas negara meliputi:

- Masalah yurisdiksi: Sulit menentukan di mana kejahatan terjadi karena sistem, pelaku, dan korban tersebar di negara berbeda.
- Anonimitas pelaku: Penggunaan VPN, TOR, dan cryptocurrency membuat pelaku nyaris tidak

terlacak.

- Minimnya kerja sama internasional: Perbedaan sistem hukum dan rendahnya kepercayaan antarnegara menghambat pertukaran informasi intelijen.
- Tidak adanya lembaga pemaksa global: Belum ada otoritas internasional yang dapat menuntut negara bertanggung jawab atas kejahatan siber lintas negara.

Kerja Sama Global dan Tanggapan Internasional

Pasca serangan WannaCry, beberapa langkah strategis telah diambil:

- Europol membentuk J-CAT (Joint Cybercrime Action Taskforce) yang berfungsi sebagai pusat koordinasi penegak hukum siber di Eropa dan mitra internasional seperti FBI dan NCA.
- Interpol dan UNODC memperluas kerja sama teknis, investigasi bersama, dan pelatihan penanganan insiden.
- Microsoft dan Cisco aktif merilis patch, mendeteksi server command-and-control (C2), dan menyediakan alat dekripsi bagi korban.
- ASEAN merumuskan strategi keamanan siber regional, sementara negara seperti Indonesia membentuk Badan Siber dan Sandi Negara (BSSN) untuk memperkuat ketahanan digital nasional (Perpres No. 53 Tahun 2017; Perpres No. 28 Tahun 2021)

Implikasi WannaCry terhadap Kebijakan Siber Global

Serangan WannaCry mengubah cara negara melihat isu siber. Di Eropa, diterbitkan NIS Directive yang mewajibkan negara anggota membentuk otoritas keamanan siber, menyusun strategi nasional, dan mewajibkan pelaporan insiden dari sektor-sektor kritikal. Versi revisinya, NIS2, memperluas cakupan dan memperketat kewajiban pengamanan.

Amerika Serikat membentuk Cybersecurity and Infrastructure Security Agency (CISA) untuk menangani ancaman digital nasional. Sementara Indonesia mengembangkan kerangka kerja nasional melalui BSSN dan memperkuat tim tanggap insiden (CSIRT).

Rekomendasi Strategis

1. Mendesak terbentuknya Cybercrime Treaty PBB yang inklusif dan menghormati kedaulatan digital semua negara.
2. Meningkatkan literasi digital dan kapasitas teknis negara berkembang.
3. Mendorong kerja sama antara sektor publik dan swasta untuk mendeteksi dan menangkal ancaman bersama.
4. Mengedepankan prinsip multistakeholder dalam tata kelola ruang digital global.

IV. Simpulan Dan Saran

4.1 Simpulan

Fenomena serangan ransomware WannaCry telah membuka mata dunia bahwa kejahatan siber bukan lagi sekadar gangguan teknis, melainkan telah menjadi ancamannyata terhadapstabilitas nasional dan internasional. Kecepatan penyebaran, cakupan lintas batas, serta dampak nyata terhadap infrastruktur kritikal seperti rumah sakit, perusahaan logistik, dan layanan publik menunjukkan bahwa dunia tengah menghadapi bentuk baru dari konflik yang dilakukan tanpa peluru, tetapi dengan kode dan celah keamanan

Melalui pendekatan yuridis-normatif dan studi kasus WannaCry, artikel ini menegaskan bahwa hukum internasional saat ini masih belum sepenuhnya siap menjawab kompleksitas kejahatan siber. Instrumen yang ada seperti Konvensi Budapest memang memberikan kerangka awal, tetapi belum mencakup seluruh komunitas internasional, dan belum memiliki mekanisme penegakan yang kuat. Di sisi lain, prinsip-prinsip hukum internasional publik seperti due diligence atau tanggung jawab negara, masih sulit diterapkan secara efektif dalam konteks kejahatan digital yang dilakukan secara anonim dan tersembunyi.

Kendala yurisdiksi, keterbatasan bukti digital, hingga perbedaan sistem hukum antarnegara menambah tantangan dalam mewujudkan pertanggungjawaban pelaku dan perlindungan korban. Hal ini diperparah oleh belum adanya konsensus global tentang definisi dan batas-batas kejahatan siber, serta kecenderungan negara-negara besar mempertahankan kedaulatan digital masing-masing.

Namun demikian, respons global terhadap WannaCry menunjukkan adanya perkembangan positif. Terbentuknya kerja sama internasional seperti J-CAT oleh Europol, peningkatan koordinasi melalui Interpol, serta partisipasi aktif sektor swasta seperti Microsoft menandakan bahwa pendekatan multistakeholder mulai terbentuk. Di tingkat kawasan, ASEAN telah menunjukkan komitmen melalui strategi kerja sama keamanan siber, sementara Uni Eropa dan Amerika Serikat bahkan telah menetapkan kebijakan digital yang tegas dan progresif.

4.2 Saran

Kasus WannaCry juga telah mendorong transformasi besar dalam kebijakan keamanan digital banyak negara. Keamanan siber kini ditempatkan sebagai prioritas nasional, setara dengan pertahanan fisik dan keamanan energi. Negara-negara mulai menerapkan prinsip zero-trust, membentuk lembaga khusus keamanan digital, serta mewajibkan pelaporan insiden siber secara reguler. Di Indonesia sendiri, pembentukan BSSN adalah langkah penting dalam memperkuat ketahanan siber nasional,

meski masih membutuhkan penguatan kapasitas dan sinergi lintas sektor.

Ke depan, tantangan terbesar bukan hanya membangun sistem pertahanan digital, tetapi juga membentuk tata kelola hukum internasional yang adil, adaptif, dan responsif terhadap perubahan zaman. Dunia membutuhkan perjanjian internasional yang mampu menjawab kebutuhan zaman digital—perjanjian yang tidak hanya melindungi sistem, tetapi juga hak-hak pengguna dan prinsip-prinsip kedaulatan dalam dunia maya.

Dengan demikian, WannaCry bukan hanya tragedi digital, tetapi juga momen refleksi global. Ia menjadi pengingat bahwa di tengah dunia yang semakin terhubung, keamanan digital adalah tanggung jawab bersama seluruh bangsa dan aktor global. Tanpa kerja sama internasional yang erat dan sistem hukum yang kuat, dunia akan tetap berada dalam bayang-bayang ancaman siber yang tak kasatmata namun sangat nyata

DAFTAR PUSTAKA

Alma Syafira (2020) Analisis Ransomware WannaCry dan Implementasinya (Skripsi, Universitas Islam Indonesia). https://dspace.uii.ac.id/bitstream/123456 789/29149/17323047-Alma-Syafira.pdf

BBC News (2017) WannaCry: What Happened During the Attack and How It Spread So Fast. https://www.bbc.com/news/technology-39901382

Citra Hardianti (2023) Kerjasama Indonesia–Korea Selatan dalam Mempertahankan Keamanan Siber Nasional di Indonesia (Poltek SSN & KOICA). https://repositori.uin-alauddin.ac.id/25857/1/30800119096_CI TRA%20HARDIANTI.pdf

Council of Europe (2001) Convention on Cybercrime (ETS No. 185). Budapest. https://www.coe.int/en/web/cybercrime/ the-budapest-convention

Fakultas Ekonomi Unesa (2023) Ransomware: Ancaman Serius bagi Keamanan Digital. BisnisDigital FEB Unesa. https://bisnisdigital.feb.unesa.ac.id/post/ ransomware-ancaman-serius-bagi-keamanan-digital

Greenberg, A (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired Magazine. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Ridwan, A (2020) Cybercrime dan Penegakan Hukum di Era Digital. Jakarta: Prenadamedia Group

Schmitt, M (Ed.) (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare.

Cambridge: Cambridge University Press UI Library (2020) Faktor-faktor Penyebab Kejahatan Ransomware, Studi pada RS Dharmais Jakarta (Tesis). https://lib.ui.ac.id/detail?id=20479326

UNODC (2021) The Global Threat of Cybercrime: Trends and Responses. United Nations Office on Drugs and Crime. https://www.unod