Jurnal Sosial dan Sains (SOSAINS)
p-ISSN 2774-7018 e-ISSN 2774-700x

Kajian Hukum Humaniter Internasional Mengenai Perang Siber Dalam Kaitannya Dengan Serangan Infrastruktur Kritis

M. Imasfy, Akhmad Alif, Tarsisius Susilo, Budiman Marpaung, Budi Saroso
Sesko TNI, Indonesia
Email: masfy9952@gmail.com, akhmadalif45@gmail.com, muchus70@gmail.com, budimanmarpaungg@gmail.com, budirowopening01@gmail.com

Abstrak

Kerentanan infrastruktur kritis terhadap serangan siber yang dampaknya setara dengan perang kinetik mengekspos kesenjangan regulasi dalam HHI, terutama terkait ketidakpastian penerapan prinsip pembedaan, proporsionalitas, dan kehati-hatian. Penelitian ini mengidentifikasi kebutuhan standar hukum baru untuk melindungi warga sipil dan infrastruktur vital di ranah digital melalui analisis tantangan penerapan HHI dalam konteks siber. Penelitian ini menggunakan metode kualitatif dengan studi dokumentasi terhadap instrumen HHI (Konvensi Jenewa 1949, Protokol Tambahan I), doktrin hukum, dan kasus serangan siber (misalnya Stuxnet). Prinsip HHI dapat diterapkan pada serangan siber, tetapi terhambat oleh sifat dual-use infrastruktur, efek berantai yang tak terprediksi, anonimitas pelaku, dan ambigu definisi "serangan" non-fisik. Diperlukan pengembangan kriteria objek siber, alat pemodelan dampak, peningkatan atribusi pelaku, dan kolaborasi global untuk memastikan HHI tetap relevan di era digital.

Keywords: Hukum Humaniter Internasional, Perang Siber, dan Serangan Infrastruktur Kritis

Abstract

The vulnerability of critical infrastructure to cyberattacks whose impact is equivalent to kinetic warfare exposes regulatory gaps in HHI, especially related to the uncertainty of applying the principles of differentiation, proportionality, and prudence. This research identifies the need for new legal standards to protect civilians and vital infrastructure in the digital realm through an analysis of the challenges of implementing HHI in a cyber context. This research uses a qualitative method with a literature study of HHI instruments (1949 Geneva Convention, Additional Protocol I), legal doctrine, and cases of cyberattacks (e.g. Stuxnet). The principles of HHI can be applied to cyberattacks, but are hampered by the dual-use nature of the infrastructure, unpredictable chain effects, the anonymity of the perpetrators, and the ambiguous definition of non-physical "attacks". The development of cyber object criteria, impact modeling tools, increased attribution of perpetrators, and global collaboration is needed to ensure that HHI remains relevant in the digital age.

Keywords: *International Humanitarian Law, Cyber Warfare, and Critical Infrastructure Attacks*

PENDAHULUAN

Transformasi global menuju era digital telah membawa perubahan fundamental dalam berbagai aspek kehidupan manusia, termasuk pergerakan dan pertukaran informasi yang kini didominasi oleh platform digital. Fenomena ini telah melahirkan ruang siber (cyberspace) sebagai matra baru yang signifikan, sejajar dengan matra tradisional seperti darat, laut, udara, dan ruang angkasa. Namun, perkembangan pesat ini tidak luput dari sisi negatif, di mana teknologi komputer dan internet disalahgunakan untuk tujuan yang menyimpang dari norma hukum demi merugikan pihak lain. Lingkungan siber yang tanpa batas ini menjadi arena baru bagi tindakan destruktif, seperti serangan siber (cyberattacks), yang memiliki potensi merusak dengan mengubah, mengganggu, menutup akses, mengurangi kinerja, atau bahkan menghancurkan file, jaringan, atau komputer itu sendiri.

Dalam konteks konflik dan keamanan, perkembangan teknologi informasi dan komunikasi telah memunculkan bentuk perang modern yang dikenal sebagai perang siber (cyber warfare) atau operasi siber (cyber operations). Perang siber didefinisikan sebagai bentuk operasi siber, baik menyerang maupun bertahan, yang dilakukan dengan tujuan untuk menyebabkan cedera atau kematian manusia, atau kerusakan atau kehancuran objek sasaran atau target operasi. Penggunaan perang siber telah dipraktikkan oleh negara-negara maju dalam konflik bersenjata, seperti yang terlihat dalam konflik internasional antara Israel dan Palestina di Gaza.

Salah satu sasaran potensial yang sangat rentan dalam perang siber adalah infrastruktur kritis suatu negara. Infrastruktur kritis mencakup sistem dan aset (fisik maupun virtual) yang vital bagi berfungsinya suatu negara dan masyarakat, di mana kegagalannya akan berdampak besar pada keamanan nasional, perekonomian, kesehatan, atau keselamatan publik (definisi umum infrastruktur kritis). Serangan siber terhadap infrastruktur kritis, seperti jaringan listrik, sistem transportasi, fasilitas keuangan, atau komunikasi, dapat menimbulkan konsekuensi yang sangat serius, termasuk gangguan layanan publik yang esensial, kerugian ekonomi masif, bahkan risiko cedera fisik atau kematian bagi masyarakat sipil akibat terganggunya layanan darurat atau fasilitas medis. Dampak yang ditimbulkan oleh serangan siber semacam ini berpotensi setara atau bahkan melebihi dampak yang dihasilkan oleh operasi kinetik tradisional, sehingga relevan untuk dikaji dalam kerangka hukum humaniter internasional.

Permasalahan mendasar timbul karena terjadi kesenjangan (gap) antara harapan atau kondisi yang seharusnya (das sollen) dan kondisi nyata atau fakta yang ada (das sein) dalam pengaturan hukum. Kondisi yang seharusnya, dalam konteks perang siber yang melibatkan target infrastruktur kritis dan berpotensi menimbulkan dampak setara dengan perang kinetik, adalah adanya kerangka hukum yang jelas dan mengikat untuk mengatur perilaku negara dan melindungi korban, sebagaimana prinsip-prinsip dasar hukum humaniter internasional seperti prinsip pembedaan, proporsionalitas, dan tindakan pencegahan. Namun, fakta yang ada (das sein), sebagaimana ditunjukkan oleh penelitian terdahulu, adalah bahwa hukum humaniter internasional hingga saat ini belum memiliki instrumen hukum yang mengikat secara khusus mengenai operasi siber dan perang siber. Meskipun hukum humaniter internasional dapat berlaku, keberlakuannya bergantung pada syarat bahwa dampak operasi tersebut setara dengan operasi kinetik, dan belum ada ketentuan spesifik yang merumuskan perang siber secara khusus. Kesenjangan ini menciptakan ketidakpastian hukum mengenai penerapan prinsip-prinsip hukum humaniter internasional terhadap serangan siber terhadap infrastruktur kritis, serta

bentuk perlindungan yang diberikan bagi masyarakat sipil yang rentan terhadap gangguan dan kerusakan yang diakibatkan oleh serangan semacam itu.

Oleh karena itu, penting untuk memahami tantangan yang muncul ketika menetapkan batasan hukum dalam dunia maya yang berubah cepat. Dengan menganalisis dampak serangan siber terhadap masyarakat sipil dan potensi pelanggaran hukum yang terjadi akibat kesenjangan regulasi, kajian ini menjadi relevan dan mendesak.

Artikel ini bertujuan untuk mengidentifikasi kebutuhan akan standar hukum baru dalam hukum humaniter internasional terkait perang siber, khususnya dalam kaitannya dengan serangan terhadap infrastruktur kritis. Identifikasi ini diharapkan dapat membantu dalam mengembangkan upaya untuk melindungi individu dan struktur kritis di ranah digital saat ini. Penelitian ini memperbarui diskusi tentang penerapan Hukum Humaniter Internasional (HHI) dalam konteks serangan siber terhadap infrastruktur kritis dengan mengeksplorasi tantangan-tantangan spesifik yang belum sepenuhnya diatasi dalam literatur sebelumnya, seperti kompleksitas infrastruktur siber yang bersifat dual-use dan kesulitan dalam menerapkan prinsip pembedaan (Miko Aditiya Suharto, 2021; Yohana Tri Meiliyanti, 2019), dampak berjenjang yang sulit diprediksi dalam penilaian proporsionalitas (ICRC, 1987; Melzer, 2011), ambiguitas definisi "serangan" siber yang bersifat non-fisik serta tantangan akuntabilitas terhadap pelaku anonim (Tallinn Manual 2.0; Clark, 2010), serta pentingnya solusi multidisiplin yang mencakup aspek hukum, teknologi, dan kebijakan untuk mengisi kesenjangan regulasi yang ada (Hollis, 2008; Kuehl, 2009).

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif karena dianggap paling sesuai untuk melakukan kajian, analisis, dan interpretasi terhadap norma-norma hukum humaniter internasional dalam konteks yang kompleks dan berkembang seperti perang siber. Metode ini memungkinkan peneliti untuk mendalami substansi hukum, mengidentifikasi prinsip-prinsip relevan, menelaah praktik negara, dan mengkonstruksikan argumentasi hukum terkait penerapan IHL di ranah siber, khususnya yang berkaitan dengan serangan terhadap infrastruktur kritis. Dengan demikian, penggunaan metode kualitatif memfasilitasi penggalian fakta hukum dan argumentasi yang lebih tuntas, pasti, dan kredibel terkait status hukum serangan siber terhadap infrastruktur kritis di bawah IHL, sesuai tujuan penelitian.

Pengumpulan data utama dalam penelitian ini dilakukan melalui studi dokumentasi atau studi kepustakaan hukum. Teknik ini dipilih karena sumber data primer dalam penelitian hukum normatif adalah norma hukum itu sendiri, yang terkandung dalam berbagai dokumen dan literatur. Studi dokumentasi memungkinkan peneliti untuk mengumpulkan dan menganalisis informasi dari berbagai sumber hukum dan non-hukum yang relevan.

Sumber data yang digunakan dalam studi dokumentasi ini meliputi:

a. Sumber Hukum Primer: Meliputi instrumen hukum internasional seperti Konvensi-Konvensi Jenewa 1949 dan Protokol-Protokol Tambahannya, serta prinsip-prinsip hukum kebiasaan internasional sebagaimana tercermin dalam praktik negara, opinio juris, dan kodifikasi oleh badan-badan ahli (misalnya, Manual Tallinn).
b. Sumber Hukum Sekunder: Meliputi doktrin hukum (karya ilmiah, buku, artikel jurnal, publikasi ahli), laporan organisasi internasional atau kelompok ahli, pernyataan resmi negara terkait posisi hukum mereka, serta putusan pengadilan internasional atau nasional jika tersedia dan relevan.

c. Dokumen Pendukung: Meliputi laporan insiden siber (yang bersifat publik), analisis teknis terkait serangan siber terhadap infrastruktur kritis (dari sumber tepercaya), dan dokumen lain yang dapat memberikan konteks atau pemahaman mengenai fenomena perang siber dan dampaknya terhadap infrastruktur kritis.

Studi dokumentasi ini bertujuan untuk memvalidasi dan mengaitkan berbagai norma hukum dengan fenomena serangan siber terhadap infrastruktur kritis, guna merumuskan analisis hukum yang komprehensif dan mendalam.

HASIL DAN PEMBAHASAN

Prinsip-prinsip dasar Hukum Humaniter Internasional (HHI), seperti prinsip pembedaan, proporsionalitas, dan kehati-hatian, dapat diterapkan secara efektif pada serangan siber terhadap infrastruktur kritis

Penerapan prinsip-prinsip dasar Hukum Humaniter Internasional (HHI) terhadap serangan siber, khususnya yang menargetkan infrastruktur kritis, merupakan isu kompleks yang muncul seiring perkembangan teknologi dan metode peperangan. HHI, yang juga dikenal sebagai hukum konflik bersenjata (jus in bello), bertujuan untuk membatasi cara dan sarana peperangan serta melindungi mereka yang tidak atau sudah tidak berpartisipasi dalam permusuhan. Meskipun HHI dikembangkan sebelum munculnya ruang siber, prinsip-prinsip dasarnya dianggap relevan dan berlaku dalam konteks konflik bersenjata yang melibatkan operasi siber, sesuai dengan prinsip bahwa hukum yang ada berlaku untuk bentuk-bentuk perang baru kecuali ada hukum yang secara eksplisit mengecualikannya.

Teori dan peraturan HHI yang relevan dalam konteks ini terutama terkandung dalam Konvensi-Konvensi Jenewa 1949 dan Protokol Tambahan I tahun 1977 (API). Prinsip-prinsip utama yang relevan adalah:

a. Prinsip Pembedaan (Principle of Distinction):

Peserta konflik harus selalu membedakan antara kombatan dan penduduk sipil, serta antara objek militer dan objek sipil. Serangan hanya boleh diarahkan pada kombatan dan objek militer. Objek militer didefinisikan sebagai objek yang, berdasarkan sifat, lokasi, tujuan, atau penggunaannya, memberikan kontribusi efektif terhadap aksi militer dan penghancuran, perebutan, atau netralisasinya, dalam keadaan yang berlaku pada saat itu, menawarkan keuntungan militer yang pasti.

Kemampuan untuk secara akurat mengidentifikasi apakah komponen siber atau sistem yang ditargetkan dalam infrastruktur kritis merupakan objek militer yang sah atau objek sipil, mengingat sifat ganda (dual-use) dari banyak sistem siber (misalnya, jaringan energi, komunikasi, atau keuangan yang digunakan oleh militer dan sipil).

Serangan siber seringkali menargetkan sistem yang memiliki fungsi ganda. Misalnya, jaringan listrik menyediakan daya untuk pangkalan militer tetapi juga untuk rumah sakit, perumahan, dan industri sipil. Menentukan apakah seluruh jaringan atau bagian darinya memenuhi definisi "objek militer" (kontribusi efektif pada aksi militer dan keuntungan militer yang pasti) adalah sulit. Kerusakan atau gangguan pada komponen "sipil" dari sistem ganda ini dapat dianggap sebagai kerusakan pada objek sipil. Prinsip pembedaan menuntut bahwa serangan siber tidak boleh diarahkan pada objek sipil, yang menimbulkan pertanyaan apakah serangan siber yang hanya mengakibatkan gangguan penggunaan sipil dari sistem ganda, tanpa secara fisik merusak komponen yang digunakan militer, merupakan serangan yang sah. Tantangan utama adalah bagaimana menerapkan konsep objek

militer pada entitas siber yang abstrak dan terkoneksi.

b. Prinsip Proporsionalitas (Principle of Proportionality):

Melarang serangan yang diperkirakan akan menyebabkan kerugian insidental terhadap kehidupan sipil, cedera pada penduduk sipil, kerusakan pada objek sipil, atau gabungan dari kerugian dan kerusakan tersebut, yang berlebihan dibandingkan dengan keuntungan militer konkret dan langsung yang diantisipasi. Prinsip ini menekankan pada kemampuan untuk memprediksi secara masuk akal potensi kerugian insidental terhadap penduduk sipil dan objek sipil akibat serangan siber terhadap infrastruktur kritis (termasuk efek berantai atau cascading effects) dan menimbangnya secara proporsional terhadap keuntungan militer yang diharapkan.

Dampak serangan siber pada infrastruktur kritis seringkali sulit diprediksi sepenuhnya dan dapat menyebar secara tak terduga melintasi sektor-sektor (misalnya, serangan terhadap jaringan energi dapat mengganggu pasokan air, layanan kesehatan, dan komunikasi). Menghitung atau memperkirakan jumlah korban sipil potensial atau tingkat kerusakan sipil dari efek berantai ini jauh lebih sulit daripada memperkirakan dampak fisik dari serangan kinetik. Keuntungan militer dari serangan siber juga mungkin sulit diukur atau dibandingkan secara langsung dengan kerugian sipil yang diperkirakan. Prinsip proporsionalitas menuntut pembatalan serangan jika kerugian sipil yang diperkirakan jelas berlebihan dibandingkan keuntungan militer. Ketidakpastian dalam memprediksi dampak siber membuat penilaian ini sangat menantang dan berpotensi membatasi jenis serangan siber tertentu terhadap infrastruktur kritis yang dampaknya luas dan tak terkendali.

c. Prinsip Kehati-hatian (Principle of Precautions in Attack):

Dalam merencanakan dan melaksanakan serangan, pihak-pihak yang terlibat dalam konflik harus mengambil semua tindakan pencegahan yang layak untuk menghindari atau setidaknya meminimalkan kerugian terhadap penduduk sipil dan objek sipil. Ini termasuk melakukan segala sesuatu yang layak dilakukan untuk memverifikasi bahwa sasaran yang akan diserang bukanlah objek sipil dan memilih sarana serta metode serangan yang, di antara pilihan yang tersedia, diperkirakan menyebabkan kerugian paling sedikit bagi penduduk sipil dan objek sipil. Prinsip ini menekankan pada kemampuan dan kesediaan pihak penyerang untuk mengambil semua tindakan pencegahan yang layak (feasible) sebelum dan selama serangan siber terhadap infrastruktur kritis untuk menghindari atau meminimalkan kerugian sipil.

Penerapan kehati-hatian dalam operasi siber mencakup beberapa aspek. Pertama, verifikasi target: apakah penyerang mengambil langkah yang layak untuk memastikan bahwa target infrastruktur kritis benar-benar merupakan objek militer atau setidaknya digunakan untuk tujuan militer? Kedua, pilihan sarana dan metode: apakah ada cara siber lain atau metode serangan yang tersedia dan layak yang dapat mencapai keuntungan militer yang sama dengan risiko minimal terhadap penduduk sipil dan objek sipil? Ketiga, peringatan: apakah layak dan efektif untuk memberikan peringatan dini sebelum melancarkan serangan siber yang dapat berdampak pada penduduk sipil? Keempat, pembatalan atau penundaan: apakah serangan dibatalkan atau ditunda jika menjadi jelas bahwa targetnya adalah sipil atau bahwa kerugian sipil akan berlebihan? Tantangan di sini adalah memastikan 'kelayakan' dalam konteks operasional siber yang seringkali membutuhkan kecepatan, kerahasiaan, dan memanfaatkan kerentanan sesaat, yang mungkin bertentangan dengan persyaratan untuk melakukan verifikasi mendalam atau

memberikan peringatan.

Tantangan yang muncul dalam menentukan status hukum subjek dan objek dalam ruang siber ketika serangan siber berdampak pada warga sipil dan layanan public.

Kajian hukum humaniter internasional (HHI) atau International Humanitarian Law (IHL) bertujuan untuk membatasi penggunaan cara dan metode perang demi mengurangi penderitaan yang disebabkan oleh konflik bersenjata. Prinsip fundamental HHI yang relevan dengan penentuan status hukum subjek dan objek dalam konflik bersenjata, termasuk potensi perang siber, meliputi:

a. Prinsip Pembedaan (Principle of Distinction): Prinsip ini mengharuskan pihak-pihak yang berkonflik untuk selalu membedakan antara kombatan dan penduduk sipil, serta antara objek militer dan objek sipil. Serangan hanya boleh diarahkan pada kombatan dan objek militer. Penduduk sipil dan objek sipil menikmati perlindungan umum dari serangan, kecuali dan untuk waktu di mana penduduk sipil secara langsung berpartisipasi dalam permusuhan atau objek sipil menjadi objek militer karena kontribusinya terhadap aksi militer. (Protokol Tambahan I Konvensi Jenewa 1949, Pasal 48, 51, 52)
b. Definisi Kombatan dan Penduduk Sipil: Kombatan umumnya adalah anggota angkatan bersenjata suatu Negara pihak dalam konflik. Penduduk sipil adalah setiap orang yang bukan kombatan. (Protokol Tambahan I Konvensi Jenewa 1949, Pasal 43, 50) Partisipasi langsung dalam permusuhan oleh penduduk sipil mengakibatkan hilangnya perlindungan dari serangan untuk waktu partisipasi tersebut. (Protokol Tambahan I Konvensi Jenewa 1949, Pasal 51(3))
c. Definisi Objek Militer dan Objek Sipil: Objek militer adalah objek yang berdasarkan sifat, lokasi, tujuan, atau penggunaannya memberikan kontribusi efektif terhadap aksi militer, dan penghancuran, penangkapan, atau netralisasi total atau parsialnya memberikan keuntungan militer yang pasti dalam keadaan yang ada pada saat itu. Semua objek yang bukan objek militer adalah objek sipil. (Protokol Tambahan I Konvensi Jenewa 1949, Pasal 52)
d. Prinsip Proporsionalitas (Principle of Proportionality): Bahkan jika suatu objek dianggap sebagai objek militer yang sah, serangan tetap dilarang jika diperkirakan akan menyebabkan kerugian insidental (kerugian tak disengaja) terhadap kehidupan sipil, luka pada penduduk sipil, atau kerusakan pada objek sipil, yang berlebihan dibandingkan dengan keuntungan militer yang pasti yang diantisipasi. (Protokol Tambahan I Konvensi Jenewa 1949, Pasal 51(5)(b))
e. Prinsip Kehati-hatian dalam Serangan (Principle of Precaution in Attack): Pihak-pihak yang berkonflik harus mengambil tindakan pencegahan yang layak untuk menghindari atau setidaknya meminimalkan kerugian terhadap penduduk sipil dan objek sipil dalam serangan. (Protokol Tambahan I Konvensi Jenewa 1949, Pasal 57)
f. Ambang Batas Konflik Bersenjata (Threshold of Armed Conflict): Agar HHI dapat berlaku sepenuhnya, harus ada konflik bersenjata. Ini bisa berupa konflik bersenjata internasional (antar negara) atau konflik bersenjata non-internasional (antara negara dan kelompok bersenjata non-negara terorganisir atau antar kelompok tersebut). Aktivitas siber dapat memicu berlakunya HHI jika mencapai ambang batas intensitas konflik bersenjata dan organisasi pihak-pihak yang terlibat.
g. Atribusi: Menentukan siapa yang bertanggung jawab atas operasi siber sangat penting. Apakah operasi tersebut dapat diatribusikan kepada suatu Negara (sebagai tindakan angkatan bersenjata atau di bawah kendali efektif Negara),

atau kepada kelompok bersenjata non-negara terorganisir? Atribusi ini menentukan apakah aturan HHI tentang konflik bersenjata internasional atau non-internasional berlaku, atau apakah insiden tersebut hanya merupakan kejahatan siber dan bukan konflik bersenjata.

Dalam konteks serangan siber yang berdampak pada warga sipil dan layanan publik (seperti serangan terhadap infrastruktur kritis), beberapa indikator muncul sebagai tantangan dalam menerapkan prinsip-prinsip HHI terkait status subjek dan objek:

a. Identifikasi Pelaku Serangan Siber (Status Subjek dan Atribusi). Ruang siber dicirikan oleh anonimitas dan kemudahan penyangkalan. Sulit untuk secara pasti mengidentifikasi siapa yang berada di balik serangan siber: apakah itu unit angkatan bersenjata Negara (kombatan), kelompok proxy yang disponsori Negara (status hukumnya bisa ambigu), kelompok peretas non-negara (yang mungkin atau mungkin tidak memenuhi syarat sebagai kelompok bersenjata terorganisir dalam NIAC), atau bahkan individu peretas (penduduk sipil). Tantangan atribusi ini secara langsung menghambat penerapan prinsip pembedaan: sulit menentukan siapa yang merupakan kombatan yang sah untuk diserang sebagai balasan, dan siapa yang merupakan penduduk sipil yang dilindungi dari serangan. Jika pelakunya tidak dapat diatribusikan kepada Negara atau kelompok bersenjata yang terlibat dalam konflik bersenjata, maka HHI tentang tata cara berperang (terkait penargetan) mungkin tidak berlaku sama sekali terhadap pelaku tersebut.
b. Indikator: Sifat Dual-Use Infrastruktur Kritis (Status Objek). Infrastruktur kritis seperti jaringan listrik, sistem pasokan air, rumah sakit, atau jaringan komunikasi memiliki sifat dual-use – mereka penting untuk kehidupan sehari-hari penduduk sipil dan penyediaan layanan publik, tetapi pada saat yang sama dapat digunakan atau mendukung operasi militer. Menerapkan definisi objek militer (yang memerlukan kontribusi efektif terhadap aksi militer dan keuntungan militer yang pasti) menjadi sangat problematik. Apakah gangguan fungsi pada jaringan listrik yang memasok listrik ke fasilitas militer dan rumah sakit sipil membuatnya menjadi objek militer yang sah? Jika iya, bagaimana memastikan serangan mematuhi prinsip proporsionalitas dan kehati-hatian, mengingat dampak besar terhadap penduduk sipil? Sulitnya menentukan apakah komponen infrastruktur kritis adalah objek militer atau sipil (atau keduanya secara simultan) secara langsung menantang penerapan prinsip pembedaan objek.
c. Partisipasi Langsung dalam Permusuhan di Ruang Siber (Status Subjek Penduduk Sipil). Prinsip pembedaan melindungi penduduk sipil kecuali jika mereka secara langsung berpartisipasi dalam permusuhan (DPH). Namun, kriteria DPH menjadi kabur di ruang siber. Apakah seorang programmer sipil yang mengembangkan kode serangan siber untuk militer berpartisipasi langsung? Apakah seorang teknisi sipil yang memelihara jaringan komputer militer berpartisipasi langsung? Bagaimana dengan sukarelawan siber yang melakukan serangan siber defensif atau ofensif terhadap sasaran militer atau sipil yang dianggap terkait dengan musuh? Ambang batas dan sifat tindakan siber yang dianggap DPH masih diperdebatkan. Ketidakjelasan ini membuat sulit untuk menentukan kapan seorang individu sipil yang terlibat dalam aktivitas siber kehilangan perlindungan dari serangan, sehingga menantang penerapan prinsip pembedaan subjek.
d. Sifat dan Efek Serangan Siber (Hubungan dengan Definisi "Serangan" dan

"Kerusakan"). Sebagaimana disinggung dalam deskripsi awal, HHI secara tradisional berkaitan dengan penggunaan kekerasan bersenjata yang menyebabkan kematian, luka-luka, atau kerusakan fisik. Serangan siber terhadap infrastruktur kritis justru seringkali menyebabkan gangguan fungsi semata tanpa kerusakan fisik permanen (misalnya, mematikan sistem kontrol industri secara sementara). Perdebatan hukum terkini, seperti yang tercermin dalam Manual Tallinn 2.0, mengindikasikan bahwa operasi siber dengan efek analog dengan serangan kinetik (menyebabkan kerusakan fisik atau cedera) dapat dianggap "serangan" di bawah HHI. Namun, gangguan fungsional murni tetap menjadi area abu-abu. Jika suatu operasi siber yang mematikan layanan publik vital (misalnya, mematikan jaringan listrik kota) tidak dianggap sebagai "serangan" di bawah HHI karena tidak ada kerusakan fisik, maka aturan HHI tentang penargetan objek sipil (termasuk infra kritis) mungkin tidak sepenuhnya berlaku, meskipun dampaknya terhadap kehidupan sipil sangat parah. Ini secara implisit menantang penerapan status objek sipil sebagai objek yang dilindungi dari "serangan".

e. Indikator: Penilaian Dampak Kemanusiaan Akibat Efek Berjenjang (Cascading Effects) (Hubungan dengan Proporsionalitas). Infrastruktur kritis saling terhubung. Serangan siber tunggal pada satu sistem (misal, energi) dapat memiliki efek berjenjang yang tidak disengaja dan sulit diprediksi ke sistem lain (misal, komunikasi, air, layanan kesehatan). Menilai kerugian sipil yang diperkirakan (untuk prinsip proporsionalitas) dan mengambil tindakan pencegahan yang layak (untuk prinsip kehati-hatian) menjadi sangat sulit dalam lingkungan siber yang kompleks dan saling bergantung. Ketidakmampuan atau kesulitan dalam secara akurat memprediksi dan menilai kerugian sipil potensial dari serangan siber (terutama pada infrastruktur sipil/dual-use) secara langsung menantang kemampuan pihak yang menyerang untuk mematuhi prinsip proporsionalitas dan kehati-hatian, sehingga meningkatkan risiko kerugian sipil dan menyulitkan penentuan apakah serangan tersebut sah secara hukum humaniter terhadap objek yang mungkin memiliki status ambigu.

Menilai dan membuktikan dampak serangan siber terhadap warga sipil dan infrastruktur kritis untuk menegakkan akuntabilitas berdasarkan HHI, mengingat sifat serangan siber yang anonim dan cepat.

Penerapan Hukum Humaniter Internasional (HHI) dalam domain siber merupakan tantangan signifikan, terutama terkait serangan siber yang menargetkan infrastruktur kritis. HHI, sebagaimana terkodifikasi dalam Konvensi Jenewa 1949 dan Protokol-Protokol Tambahannya, mengatur perilaku pihak-pihak dalam konflik bersenjata, bertujuan untuk membatasi penderitaan akibat perang. Prinsip-prinsip fundamental HHI yang relevan mencakup prinsip pembedaan (distinction), proporsionalitas (proportionality), dan kehati-hatian dalam serangan (precautions in attack). Prinsip pembedaan mewajibkan pihak yang berkonflik untuk selalu membedakan antara kombatan dan penduduk sipil, serta antara objek militer dan objek sipil. Serangan hanya boleh ditujukan terhadap objek militer. Prinsip proporsionalitas melarang serangan terhadap objek militer jika diperkirakan akan menimbulkan kerugian insidental terhadap penduduk sipil atau objek sipil yang berlebihan dibandingkan keuntungan militer yang diharapkan. Prinsip kehati-hatian mewajibkan pihak yang menyerang untuk mengambil semua langkah yang mungkin untuk menghindari, atau setidaknya meminimalisasi, kerugian terhadap warga sipil dan objek sipil.

Dalam konteks siber, serangan yang mencapai ambang batas konflik bersenjata atau yang menyebabkan efek yang sepadan dengan operasi militer konvensional harus mematuhi prinsip-prinsip HHI ini. Serangan siber terhadap infrastruktur kritis (seperti jaringan listrik, sistem pasokan air, rumah sakit, sistem perbankan) sangat sensitif terhadap HHI karena dampak langsung dan tidak langsungnya terhadap penduduk sipil. Tantangan utama muncul dalam menilai dan membuktikan dampak serangan siber terhadap warga sipil dan infrastruktur kritis untuk menegakkan akuntabilitas, mengingat sifat serangan siber yang sering kali anonim dan sangat cepat.

Beberapa indikator yang dapat digunakan untuk menilai dampak serangan siber dihadapkan pada teori HHI yang relevan mencakup:

a. Kematian atau Cedera pada Warga Sipil:

HHI secara tegas melarang serangan langsung terhadap warga sipil. Serangan siber dapat secara tidak langsung menyebabkan kematian atau cedera. Misalnya, serangan siber yang melumpuhkan sistem rumah sakit dapat mencegah pemberian bantuan medis yang vital, atau serangan pada jaringan listrik dapat menghentikan pasokan daya ke alat penunjang kehidupan medis.

Membuktikan kausalitas antara serangan siber tertentu yang anonim dan cepat dengan kematian atau cedera sipil sangat sulit. Efeknya bisa jadi tidak langsung atau tertunda. Menelusuri jalur digital dari serangan hingga dampak fisik memerlukan forensik digital yang canggih dan korelasi data medis atau insiden fisik dengan timeline serangan siber. Anonimitas mempersulit identifikasi pelaku yang dapat dimintai pertanggungjawaban atas dampak tersebut. Kecepatan serangan dapat berarti bukti digital transient hilang dengan cepat.

b. Kerusakan atau Hancurnya Objek Sipil:

HHI melindungi objek sipil dari serangan. Meskipun serangan siber mungkin tidak secara fisik merusak objek, ia dapat membuatnya tidak berfungsi, yang dalam konteks tertentu dapat dianggap setara dengan kerusakan atau hancurnya objek dalam arti fungsionalnya. Serangan terhadap sistem kontrol industri (SCADA) yang mengoperasikan pabrik air atau bendungan dapat membuat objek tersebut tidak berfungsi, bahkan jika strukturnya tetap utuh.

Seperti halnya kematian/cedera, membuktikan bahwa serangan siber spesifik yang bersifat non-fisik menyebabkan kelumpuhan fungsional suatu objek sipil (atau bagian sipil dari objek dual-use) memerlukan analisis teknis mendalam terhadap log sistem, lalu lintas jaringan, dan data operasional objek tersebut, dikorelasikan dengan waktu serangan. Menetapkan link kausal ini di tengah hiruk-pikuk serangan siber berkecepatan tinggi, seringkali dengan banyak vektor, adalah kompleks. Anonimitas menghambat penegakan tanggung jawab.

c. Dampak Berlebihan terhadap Warga Sipil (Pelanggaran Proporsionalitas):

Menilai apakah kerugian insidental terhadap warga sipil dari serangan siber terhadap objek militer (atau objek dual-use) adalah berlebihan dibandingkan keuntungan militer merupakan tantangan besar. Serangan siber dapat memiliki efek berjenjang (cascading effects) yang sulit diprediksi dan dikendalikan, meluas melampaui target awal dan mempengaruhi layanan sipil secara luas.

Menilai proporsionalitas memerlukan penilaian foreseeability (kemampuan untuk diprediksi) dampak sipil insidental sebelum serangan. Sifat efek berjenjang serangan siber membuat prediksi dampak ini sangat sulit. Setelah serangan, menilai apakah dampak sipil itu berlebihan memerlukan pengumpulan data kerugian sipil dan data teknis serangan secara komprehensif dan cepat, yang kembali dipersulit oleh anonimitas dan kecepatan. Bagaimana suatu negara atau individu dapat

dimintai pertanggungjawaban atas dampak yang tidak dapat diprediksi atau berlebihan jika pelaku serangan tidak dapat diidentifikasi atau jika bukti kausalitas yang jelas sulit ditemukan dalam waktu singkat?

d. Lumpuhnya Fungsi Infrastruktur Kritis Esensial bagi Kehidupan Sipil:

Serangan siber yang melumpuhkan infrastruktur kritis yang menopang kehidupan sehari-hari penduduk sipil (listrik, air bersih, layanan kesehatan, komunikasi) secara langsung melanggar semangat perlindungan HHI terhadap warga sipil dan objek sipil yang penting bagi kelangsungan hidup mereka. Meskipun infrastruktur semacam itu terkadang memiliki fungsi dual-use (sipil dan militer), serangannya harus tetap mematuhi prinsip pembedaan dan proporsionalitas.

Membuktikan bahwa kelumpuhan infrastruktur kritis disebabkan oleh serangan siber tertentu memerlukan penelusuran teknis yang rumit. Infrastruktur modern sangat saling terhubung; satu serangan dapat memicu kegagalan di sistem lain. Memilah penyebab spesifik (apakah siber, kegagalan internal, atau sebab lain) sambil bukti digital lenyap atau ditimpa karena kecepatan operasi siber merupakan tantangan besar. Anonimitas membuat siapa yang harus bertanggung jawab atas kerugian masif akibat lumpuhnya infrastruktur ini menjadi pertanyaan krusial.

Prinsip-prinsip dasar Hukum Humaniter Internasional (HHI), seperti prinsip pembedaan, proporsionalitas, dan kehati-hatian, dapat diterapkan secara efektif pada serangan siber terhadap infrastruktur kritis.

Berdasarkan hasil analisa di atas, prinsip-prinsip pembedaan, proporsionalitas, dan kehati-hatian memang dapat dan harus diterapkan pada serangan siber terhadap infrastruktur kritis dalam konteks konflik bersenjata. Namun, penerapannya dihadapkan pada tantangan praktis yang signifikan akibat sifat unik dari domain siber dan target infrastruktur kritis.

Permasalahan utama terletak pada kesulitan dalam mengadaptasi konsep-konsep yang dikembangkan untuk perang fisik ke dalam domain siber yang intangible, terkoneksi, dan seringkali memiliki fungsi ganda. Indikator pembedaan menunjukkan bahwa garis antara objek militer dan sipil menjadi buram ketika menyangkut sistem siber infrastruktur kritis. Definisi objek militer dalam HHI memerlukan kontribusi efektif terhadap aksi militer dan keuntungan militer yang pasti, yang sulit dinilai pada sistem yang juga secara vital menopang kehidupan sipil. Serangan terhadap bagian 'sipil' dari sistem ganda tetap dilarang sebagai serangan terhadap objek sipil.

Indikator proporsionalitas menyoroti ketidakpastian tinggi dalam memprediksi dampak serangan siber terhadap infrastruktur kritis, terutama efek berantai yang dapat melumpuhkan berbagai sektor dan menyebabkan kerugian sipil yang luas dan tidak langsung. Ketidakmampuan untuk secara akurat memprediksi kerugian insidental ini membuat penilaian proporsionalitas menjadi sangat spekulatif dan sulit, yang dapat mengakibatkan penyerang berisiko melanggar prinsip ini jika serangan dilancarkan tanpa pemahaman yang memadai tentang dampaknya.

Terakhir, indikator kehati-hatian mengungkapkan kesulitan dalam mengambil semua langkah pencegahan yang 'layak' dalam operasi siber. Persyaratan untuk memverifikasi target, memilih metode yang paling tidak merugikan, dan memberikan peringatan mungkin sulit dipenuhi dalam kecepatan dan kerahasiaan operasi siber, di mana penyerang mungkin memiliki jendela peluang yang sempit untuk mengeksploitasi kerentanan.

Meskipun tantangan ini ada, HHI tetap berlaku. Kesulitan dalam penerapan

tidak meniadakan kewajiban hukum. Sebaliknya, kesulitan ini justru menempatkan beban yang lebih berat pada penyerang untuk melakukan penilaian yang cermat dan hati-hati sebelum, selama, dan setelah serangan siber. Jika penilaian dampak sipil terlalu tidak pasti, atau jika tidak mungkin untuk membedakan target atau mengambil tindakan pencegahan yang memadai, HHI mungkin melarang dilakukannya serangan siber tertentu terhadap infrastruktur kritis, terutama yang rentan terhadap efek berantai yang luas. Dengan demikian, prinsip-prinsip HHI secara efektif bertindak sebagai batasan hukum yang penting pada serangan siber, meskipun penerapannya memerlukan interpretasi dan pemahaman yang terus berkembang.

Tantangan yang muncul dalam menentukan status hukum subjek dan objek dalam ruang siber ketika serangan siber berdampak pada warga sipil dan layanan public.

Berdasarkan hasil analisis di atas, dapat dibahas bahwa tantangan dalam menentukan status hukum subjek dan objek dalam ruang siber, khususnya ketika serangan berdampak pada warga sipil dan layanan publik, sangat kompleks dan berasal dari ketidakcocokan inheren antara kerangka hukum humaniter internasional yang dikembangkan untuk konflik kinetik dan karakteristik unik dari perang siber.

Permasalahan utama yang muncul ketika serangan siber menyasar atau berdampak pada warga sipil dan layanan publik adalah:

a. Sulitnya Mengaplikasikan Prinsip Pembedaan: Prinsip fundamental HHI ini sangat bergantung pada identifikasi jelas subjek (kombatan vs. sipil) dan objek (militer vs. sipil). Di ruang siber, anonimitas (Indikator 1) membuat atribusi serangan menjadi kabur, sehingga sulit untuk menentukan siapa pelaku yang sah ditargetkan berdasarkan status kombatannya. Sifat dual-use infrastruktur kritis (Indikator 2) mempersulit klasifikasi objek sebagai murni militer atau sipil, menantang penargetan eksklusif pada objek militer. Lebih lanjut, aktivitas siber oleh individu sipil yang mungkin berkontribusi pada upaya perang (Indikator 3) memperumit penerapan konsep Partisipasi Langsung dalam Permusuhan (DPH), memburamkan garis antara penduduk sipil yang dilindungi dan individu yang kehilangan perlindungannya. Semua ini secara kolektif menghambat kemampuan pihak-pihak yang berkonflik untuk secara efektif menerapkan prinsip pembedaan, yang merupakan pilar perlindungan sipil di bawah HHI.
b. Ketidakjelasan Definisi "Serangan" dan Kepatuhan terhadap Aturan Penargetan: Jika, seperti yang disinggung dalam teks awal, bentuk serangan siber tertentu yang menyebabkan gangguan fungsi parah pada layanan publik tetapi tanpa kerusakan fisik (Indikator 4) berada di area abu-abu dan mungkin tidak selalu dianggap "serangan" di bawah HHI, maka aturan penargetan HHI yang dirancang untuk mencegah kerugian sipil dari "serangan" mungkin tidak sepenuhnya berlaku. Ini menciptakan kesenjangan perlindungan hukum bagi penduduk sipil yang menderita akibat parah dari operasi siber tersebut, terlepas dari apakah objek yang diserang dianggap sipil atau dual-use.
c. Hambatan dalam Memenuhi Kewajiban Proporsionalitas dan Kehati-hatian: Bahkan jika suatu objek infrastruktur kritis dianggap objek militer, sifat efek siber yang berjenjang dan sulit diprediksi (Indikator 5) membuat penilaian kerugian sipil insidental menjadi sangat sulit. Ini secara langsung menantang kemampuan pihak yang menyerang untuk memenuhi kewajiban mereka di bawah prinsip proporsionalitas (memastikan keuntungan militer tidak berlebihan dibandingkan kerugian sipil) dan kehati-hatian (mengambil langkah

untuk meminimalkan kerugian). Padahal, prinsip-prinsip ini adalah mekanisme perlindungan sipil yang krusial di tengah situasi penargetan objek yang mungkin memiliki status ambigu. Dampak langsung pada warga sipil dan layanan publik justru memperlihatkan betapa sulitnya menerapkan penilaian risiko dan tindakan pencegahan dalam lingkungan siber yang kompleks.

Implikasi dari tantangan ini sangat signifikan. Jika kerangka hukum tidak jelas dapat diaplikasikan atau dipatuhi, risiko kerugian sipil yang tidak proporsional akibat operasi siber terhadap infrastruktur vital menjadi sangat tinggi.

Menilai dan membuktikan dampak serangan siber terhadap warga sipil dan infrastruktur kritis untuk menegakkan akuntabilitas berdasarkan HHI, mengingat sifat serangan siber yang anonim dan cepat.

Hasil analisa di atas menunjukkan bahwa penilaian dan pembuktian dampak serangan siber terhadap warga sipil dan infrastruktur kritis untuk tujuan akuntabilitas berdasarkan HHI sangat terhambat oleh sifat inheren serangan siber, yaitu anonimitas dan kecepatan. Konsep tradisional HHI mengenai "serangan" dan "kerusakan" yang dikembangkan dalam konteks perang konvensional (fisik) tidak selalu mudah diterapkan pada domain siber yang non-kinetik dan saling terhubung.

Masalah anonimitas secara langsung mempengaruhi kemampuan untuk menegakkan akuntabilitas, baik akuntabilitas negara maupun individu. HHI mewajibkan negara untuk menghormati dan menjamin penghormatan terhadap hukum tersebut. Jika serangan yang melanggar HHI tidak dapat diatribusikan secara pasti kepada negara atau aktor non-negara tertentu, penegakan tanggung jawab negara menjadi mustahil. Demikian pula, penuntutan pidana terhadap individu yang bertanggung jawab (misalnya, komandan atau pelaku langsung) memerlukan bukti yang kuat mengenai identitas dan perannya dalam serangan tersebut, yang sangat sulit didapatkan dalam operasi siber yang tersembunyi. Meskipun komunitas teknis seringkali dapat melakukan atribusi teknis, atribusi ini belum tentu memenuhi standar bukti hukum yang diperlukan untuk akuntabilitas negara atau pidana.

Kecepatan serangan siber dan sifat efemeral (sementara) dari banyak bukti digital menambah lapisan kesulitan dalam membuktikan kausalitas dan mengukur dampak. Pada saat dampak fisik atau fungsional serangan siber terlihat jelas (misalnya, rumah sakit tidak berfungsi atau sistem listrik padam), bukti digital yang dapat menghubungkan dampak tersebut dengan serangan spesifik mungkin sudah hilang atau sulit dipulihkan tanpa protokol insiden respons yang sangat cepat dan terkoordinasi. Men demonstrate bahwa suatu insiden adalah konsekuensi langsung dari serangan siber tertentu, dan bukan kegagalan sistem lain atau efek dari serangan siber lain—atau bahkan operasi militer konvensional memerlukan tingkat koordinasi teknis dan investigatif yang seringkali melampaui kapasitas penegakan hukum atau mekanisme pengawasan HHI yang ada.

Untuk mengatasi tantangan ini dalam rangka menegakkan akuntabilitas berdasarkan HHI, diperlukan pendekatan multi dimensi:

a. Pengembangan Kapasitas Teknis: Negara dan organisasi internasional memerlukan kemampuan forensik siber yang canggih untuk melacak asal-usul serangan, merekonstruksi rantai kausalitas dari serangan siber ke dampak fisik/fungsional, dan mengumpulkan bukti digital yang relevan sebelum hilang.
b. Kerja Sama Internasional: Anonimitas dan sifat transnasional dari serangan siber menuntut kerja sama antarnegara dalam berbagi informasi siber, intelijen, dan bukti digital untuk membantu proses atribusi dan pembuktian.
c. Klarifikasi Penerapan HHI: Komunitas internasional perlu terus

memperdebatkan dan, jika memungkinkan, mengklarifikasi bagaimana prinsip-prinsip HHI (khususnya definisi ‘serangan’, ‘objek militer’, ‘kerusakan’, dan penilaian ‘proporsionalitas’) berlaku secara spesifik dalam domain siber. Ini mungkin memerlukan pengembangan norma atau interpretasi baru.

d. Pendekatan Bukti yang Komprehensif: Mengingat sulitnya mendapatkan bukti langsung, investigasi mungkin perlu mengandalkan bukti tidak langsung atau sirkumstansial yang lebih kuat, yang dikumpulkan dari berbagai sumber (teknis, intelijen, saksi dampak, analisis operasional) untuk membangun kasus atribusi dan kausalitas.
e. Perumusan Norma Negara: Negara-negara perlu memperjelas posisi mereka mengenai penerapan HHI terhadap operasi siber dan mengembangkan praktik negara yang konsisten terkait serangan siber yang menargetkan atau mempengaruhi infrastruktur kritis.

KESIMPULAN

Prinsip-prinsip Hukum Humaniter Internasional (HHI), seperti pembedaan, proporsionalitas, dan kehati-hatian, dapat diterapkan pada serangan siber terhadap infrastruktur kritis, tetapi tantangan utamanya meliputi kesulitan membedakan objek militer-sipil dalam sistem siber *dual-use*, memprediksi dampak berjenjang (*cascading effects*), serta memenuhi kewajiban kehati-hatian dalam operasi siber yang cepat dan berbasis kerentanan sesaat. Selain itu, ambigu dalam identifikasi pelaku, atribusi serangan, dan definisi "serangan" siber (termasuk efek non-fisik) memperumit penegakan HHI. Untuk mengatasi hal ini, penelitian selanjutnya perlu fokus pada: (1) pengembangan kriteria pembedaan objek siber, (2) pemodelan dampak proporsionalitas, (3) penyesuaian prinsip kehati-hatian, (4) peningkatan metode atribusi pelaku, (5) reinterpretasi konsep "serangan" siber, (6) mekanisme penegakan hukum yang adaptif, dan (7) kolaborasi multidisiplin (hukum, teknologi, kebijakan) guna memastikan HHI tetap relevan di era digital. Pendekatan inovatif dan global diperlukan untuk menjawab kompleksitas ini, termasuk analisis kasus empiris, alat simulasi dampak, serta dialog antar-pemangku kepentingan.

REFERENCES

Miko Aditiya Suharto1, Maria Novita Apriyani. Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. Risalah Hukum, Volume 17, Nomor 2, Desember 2021, 98-107. Fakultas Hukum UPN"Veteran" Jawa Timur.

Yohana Tri Meiliyanti*, Joko Setiyono, Kabul Supriyadhie. Kajian Hukum Humaniter Internasional Mengenai Cyber Warfare Dalam Konflik Bersenjata Internasional Antara Israel Dan Palestina Atas Gaza. Volume 8, Nomor 2, Tahun 2019. Website : https://ejournal3.undip.ac.id/index.php/dlr/

ICRC, Commentary on the Additional Protocols to the Geneva Conventions of 12 August 1949, Geneva: Martinus Nijhoff Publishers, 1987, hlm. 618

Clark, David, "Characterizing Cyberspace: Past, Present And Future," MIT CSAIL, Version, 1 (2010), 2016–28

Even, Shmuel, dan Davıd Siman Ṭov, Cyber Warfare: Concepts and Strategic Trends (JSTOR, 2012)

Hollis, David, "SWJ Books | Small Wars Journal," 2008 <https://smallwarsjournal.com/index.php/books> [diakses 24 April 2025]

Kuehl, Daniel T, "From Cyberspace To Cyberpower : Defining The Problem," Cyberpower and national security, 1 (2009)

Konsep Cyber Attack, Cyber Crime, Dan Cybe Warfare (Miko Aditiya Suharto) 107

Melzer, N, "Cyberwarfare And International Law. UNIDIR Resources," UN Institute for, 2011

Wahid, Abdul, Kejahatan Mayantara (Cyber Crime) (Bandung: Refika Aditama, 2005) "What Is a Cyber Attack? | Cyber Attack Definition | Unisys" <https://www.unisys.com/glossary/cyber-attack/> [diakses 24 April 2025]

"What is a cyber attack? | IBM" <https://www.ibm.com/id-en/topics/cyber-attack> [diakses 24 April 2025]

"What Is a Cyberattack? - Most Common Types - Cisco" <https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html> [diakses 24 April 2025]