JIM: Jurnal Ilmu Multidisiplin
E-ISSN: 2829-4580
P-ISSN: 2829-4599
GREENATION PUBLISHER
+62 812 1046 7572 http://greenpub.org greenation.info@gmail.com
DOI: https://doi.org/10.38035/jim.v4i2

Dampak Kesehatan Internasional Akibat Cyber War Rusia-Ukraina

Vishnu Kusumawardhana[1*], Fitry Taufik Sahary[2], Arief Fahmi Lubis[3], Boedi Prasetyo[4]
[1]Sekolah Tinggi Hukum Militer, Jakarta, Indonesia, elang_vishnu@ymail.com
[2]Sekolah Tinggi Hukum Militer, Jakarta, Indonesia, fitryts94@gmail.com
[3]Sekolah Tinggi Hukum Militer, Jakarta, Indonesia, arieffahmilubis0@gmail.com
[4]Sekolah Tinggi Hukum Militer, Jakarta, Indonesia, boedi.prasetyo@sthm.ac.id

*Corresponding Author: elang_vishnu@ymail.com[1]

Abstract: *The cyber war between Russia and Ukraine has demonstrated a modern form of conflict that not only impacts military systems, but also civilian infrastructure including health facilities. This article examines how International Health Law and International Humanitarian Law provide protection for medical facilities in cyberwar situations. Using a qualitative normative approach, this paper analyzes the legal principles violated in cyber attacks and the challenges of implementing law in the digital realm. This article also offers solutions in the form of strengthening regulations, increasing international cooperation, and educating related actors.*

Keywords: *Cyber War, International Health Law, Russia, Ukraine, International Humanitarian Law.*

Abstrak: Perang siber antara Rusia dan Ukraina telah memperlihatkan bentuk konflik modern yang tidak hanya berdampak pada sistem militer, tetapi juga infrastruktur sipil termasuk fasilitas kesehatan. Artikel ini mengkaji bagaimana Hukum Kesehatan Internasional dan Hukum Humaniter Internasional memberikan perlindungan terhadap fasilitas medis dalam situasi perang siber. Dengan menggunakan pendekatan kualitatif normatif, tulisan ini menganalisis prinsip-prinsip hukum yang dilanggar dalam serangan siber serta tantangan implementasi hukum di ranah digital. Artikel ini juga menawarkan solusi berupa penguatan regulasi, peningkatan kerja sama internasional, serta edukasi terhadap aktor-aktor terkait.

Kata Kunci: Perang Siber, Hukum Kesehatan Internasional, Rusia, Ukraina, Hukum Humaniter.

PENDAHULUAN

Perang siber telah berkembang menjadi elemen strategis dalam konflik bersenjata modern, menggantikan sebagian besar pendekatan konvensional dengan serangan berbasis digital yang dapat melumpuhkan infrastruktur penting tanpa kehadiran fisik. Salah satu konflik yang memperlihatkan intensitas dan kompleksitas perang siber adalah perang antara

Rusia dan Ukraina yang dimulai sejak 2014 dan memuncak pada 2022. Di luar dampak terhadap sistem militer dan pemerintahan, serangan siber juga menyasar sektor-sektor sipil yang krusial, termasuk sistem kesehatan.

Fasilitas kesehatan, yang secara hukum harus dilindungi selama konflik, telah menjadi target dalam berbagai bentuk serangan digital. Ini meliputi peretasan terhadap sistem informasi rumah sakit, pemadaman perangkat medis yang tersambung secara daring, serta penyebaran malware yang menghambat layanan kesehatan. Serangan ini tidak hanya melanggar norma etika, tetapi juga menimbulkan pertanyaan penting terkait kepatuhan terhadap Hukum Humaniter Internasional (HHI) dan Hukum Kesehatan Internasional.

Oleh karena itu, presentasi ini bertujuan untuk mengkaji bagaimana kerangka hukum internasional memberikan perlindungan terhadap fasilitas dan tenaga medis dalam konteks perang siber. Fokus akan diarahkan pada prinsip-prinsip utama dalam HHI, seperti netralitas, proporsionalitas, dan kemanusiaan, serta bagaimana prinsip-prinsip tersebut diterapkan atau dilanggar dalam kasus konflik Rusia‑Ukraina. Di samping itu, pembahasan juga mencakup tantangan aktual dalam implementasi hukum, seperti kesulitan atribusi, yurisdiksi, dan pengumpulan bukti digital.

Dengan pendekatan normatif dan analitis, diharapkan pembahasan ini dapat memberikan kontribusi terhadap penguatan instrumen hukum dan kebijakan global dalam melindungi sistem kesehatan dari ancaman perang siber di masa depan.

METODE

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan kualitatif, yaitu menelaah prinsip dan norma hukum internasional yang relevan terhadap perlindungan fasilitas kesehatan dalam konteks perang siber Rusia–Ukraina. Data diperoleh dari bahan hukum sekunder seperti perjanjian internasional, dokumen organisasi internasional, jurnal ilmiah, dan laporan konflik, yang dianalisis secara deskriptif untuk mengidentifikasi pelanggaran hukum dan solusi kebijakan yang mungkin diterapkan.

HASIL DAN PEMBAHASAN

Definisi dan Ruang Lingkup Cyber War

Definisi Cyber War

Cyber war atau perang siber adalah konflik yang terjadi di ranah siber, melibatkan penggunaan teknologi informasi untuk menyerang atau merusak sistem dan infrastruktur musuh. Ini mencakup serangan terhadap sistem komputer, jaringan, dan data yang vital bagi fungsi negara dan masyarakat. Perang siber tidak terbatas pada tindakan perusakan fisik, tetapi juga termasuk operasi yang bertujuan untuk mencuri informasi, menyebarkan disinformasi, atau mengganggu proses komunikasi musuh. Serangan ini sering bersifat tersembunyi dan sulit dideteksi, sehingga memperumit upaya pertahanan dan penegakan hukum. Dalam konteks militer, perang siber dapat melemahkan kemampuan operasional lawan tanpa perlu penggunaan senjata konvensional, sehingga menjadi alat strategis yang semakin penting dalam konflik modern

Ruang Lingkup Cyber War dalam Konflik Rusia-Ukraina

Dalam konteks konflik Rusia–Ukraina, perang siber telah menjadi instrumen utama dalam strategi militer dan non-militer. Rusia, sebagai aktor dominan, telah melancarkan berbagai serangan siber sejak aneksasi Krimea tahun 2014, yang kemudian meningkat secara signifikan sejak invasi besar-besaran pada Februari 2022. Perang siber ini mencakup tindakan sabotase terhadap infrastruktur kritis seperti jaringan listrik, sistem transportasi, dan layanan publik. Salah satu aspek yang paling mengkhawatirkan dari perang siber ini adalah menyasar sektor kesehatan. Fasilitas medis, sistem informasi rumah sakit, dan data pasien menjadi target serangan, mengakibatkan gangguan layanan, kehilangan data vital, serta ancaman

terhadap keselamatan pasien. Ini menunjukkan bahwa perang siber tidak lagi terbatas pada dimensi strategis atau militer, tetapi telah memasuki ranah kemanusiaan.

Lebih lanjut, perang siber juga digunakan sebagai sarana perang psikologis dan penyebaran disinformasi. Melalui media sosial dan platform daring lainnya, pihak-pihak yang terlibat dalam konflik menyebarkan informasi palsu untuk memanipulasi opini publik, menciptakan ketakutan, dan melemahkan kepercayaan terhadap institusi kesehatan. Ini secara langsung bertentangan dengan prinsip-prinsip Hukum Humaniter Internasional (HHI), khususnya mengenai perlindungan terhadap warga sipil dan infrastruktur sipil.

Dengan semakin terintegrasinya teknologi dalam sistem kesehatan, ruang lingkup perang siber di masa kini menuntut pemahaman hukum yang lebih luas dan respons internasional yang lebih tegas untuk menjamin perlindungan terhadap hak atas kesehatan dan keselamatan selama konflik bersenjata digital.

Perlindungan Fasilitas Kesehatan dalam Hukum Humaniter Internasional

1. Perlindungan Kesehatan

   Hukum Humaniter Internasional (HHI) memberikan perlindungan khusus kepada fasilitas kesehatan selama konflik bersenjata. Pasal 18 Konvensi Jenewa IV dan Pasal 12 serta Pasal 15 Protokol Tambahan I menegaskan bahwa fasilitas medis, personel kesehatan, dan transportasi medis harus dihormati dan dilindungi dari segala bentuk serangan dan gangguan. Perlindungan ini juga mencakup larangan penargetan langsung fasilitas kesehatan, kecuali jika fasilitas tersebut digunakan untuk tujuan militer secara langsung dan sah menurut hukum internasional. Selain itu, HHI mengatur kewajiban semua pihak dalam konflik untuk mengambil langkah-langkah pencegahan guna meminimalkan dampak pada fasilitas kesehatan serta menjamin akses yang aman dan tidak terhalang bagi pasien dan tenaga medis
2. Larangan Serangan

   Hukum Humaniter Internasional secara tegas melarang serangan terhadap fasilitas kesehatan selama konflik bersenjata, sebagaimana diatur dalam Protokol Tambahan I terhadap Konvensi Jenewa tahun 1977. Namun, larangan ini memiliki pengecualian terbatas: serangan dapat dilakukan hanya jika fasilitas kesehatan tersebut digunakan untuk melakukan tindakan yang merugikan pihak lawan, seperti menyembunyikan senjata atau melancarkan operasi militer. Akan tetapi, meskipun terdapat indikasi penyalahgunaan fungsi fasilitas kesehatan, hukum tetap mewajibkan adanya peringatan sebelumnya dan memberikan waktu yang cukup untuk menghentikan aktivitas tersebut. Jika serangan tetap dilakukan, maka prinsip proporsionalitas dan kehati-hatian (precaution) wajib diterapkan untuk meminimalkan korban sipil dan kerusakan yang tidak perlu. Dengan demikian, penyerangan terhadap fasilitas kesehatan harus menjadi upaya terakhir yang sangat dibatasi oleh kerangka hukum internasional yang ketat.
3. Tanggung Jawab Negara

   Dalam kerangka Hukum Humaniter Internasional (HHI), negara memiliki tanggung jawab hukum yang tegas untuk memastikan bahwa seluruh unsur pasukannya menghormati dan mematuhi aturan perlindungan terhadap fasilitas kesehatan. Hal ini mencakup kewajiban untuk memberikan pelatihan dan instruksi hukum kepada militer mengenai larangan menyerang fasilitas medis, serta menjamin penegakan hukum melalui mekanisme investigasi dan peradilan bagi mereka yang diduga melakukan pelanggaran. Negara juga bertanggung jawab secara internasional apabila terbukti gagal mencegah, menghukum, atau mengatasi pelanggaran serius terhadap HHI oleh aparat atau individu yang berada di bawah yurisdiksinya. Prinsip pertanggungjawaban ini diperkuat dalam Statuta Roma Mahkamah Pidana Internasional (1998), yang mengklasifikasikan serangan yang disengaja terhadap rumah sakit dan fasilitas medis sipil sebagai kejahatan perang.

Oleh karena itu, tanggung jawab negara bukan hanya bersifat moral, melainkan juga legal dan dapat dimintakan akuntabilitasnya melalui forum hukum internasional.

Dampak Cyber War terhadap Sistem Kesehatan Ukraina

1. Gangguan Layanan

   Serangan siber telah menyebabkan gangguan signifikan terhadap layanan kesehatan di Ukraina, termasuk pembatalan janji temu, penundaan prosedur medis, dan kesulitan dalam mengakses catatan pasien. Gangguan ini mengakibatkan penurunan efektivitas sistem kesehatan secara keseluruhan karena koordinasi antar unit medis menjadi terhambat, serta keterlambatan dalam penanganan pasien kritis meningkat. Selain itu, serangan ini memicu kekhawatiran terkait keamanan data dan keandalan sistem informasi rumah sakit, yang secara langsung mempengaruhi kualitas pelayanan medis yang diberikan. Dampak ini juga mengakibatkan tekanan psikologis bagi tenaga kesehatan yang berusaha bekerja dalam kondisi penuh ketidakpastian dan risiko tinggi akibat gangguan teknologi.
2. Pelanggaran Data

   Serangan terhadap sistem informasi rumah sakit dan fasilitas kesehatan lainnya telah mengakibatkan pelanggaran data sensitif pasien. Data medis yang bocor atau dicuri dapat meliputi rekam medis, identitas pribadi, dan informasi terkait pengobatan. Pelanggaran ini tidak hanya melanggar privasi dan hak-hak pasien, tetapi juga membuka peluang bagi pelaku kejahatan siber untuk melakukan pemerasan (ransomware), penipuan asuransi, dan diskriminasi berbasis data kesehatan. Selain itu, kebocoran data medis dapat mengganggu kepercayaan masyarakat terhadap sistem kesehatan dan memperburuk krisis kesehatan di tengah konflik. Perlindungan data pasien menjadi aspek penting yang harus diakomodasi dalam kebijakan keamanan siber di sektor kesehatan, terutama di negara yang menghadapi ancaman perang siber seperti Ukraina
3. Ancaman Terhadap Peralatan Medis

   Peralatan medis yang terhubung ke jaringan, seperti monitor jantung**,** ventilator**,** pompa infus, serta sistem pencitraan medis (MRI, CT scan), merupakan komponen vital dalam pelayanan kesehatan modern. Konektivitas perangkat ini dengan sistem teknologi informasi rumah sakit menjadikan mereka bagian dari ekosistem "Internet of Medical Things" (IoMT), yang sekaligus membuka celah bagi serangan siber yang bersifat merusak.

   Dalam konteks perang siber Rusia‑Ukraina, terdapat laporan gangguan sistem di rumah sakit yang menyebabkan tertundanya prosedur medis atau kegagalan perangkat yang dibutuhkan dalam situasi darurat. Serangan ransomware, misalnya, dapat mengunci sistem operasi peralatan dan meminta tebusan, sementara serangan malware dapat memodifikasi fungsi perangkat secara diam-diam. Jika serangan tersebut terjadi saat alat sedang digunakan untuk pasien kritis, konsekuensinya bisa berakibat fatal, seperti kegagalan deteksi ritme jantung atau gangguan pada ventilasi mekanik.

   Selain itu, sistem pencitraan medis yang terganggu dapat menghasilkan data yang tidak akurat atau bahkan tidak dapat diakses, menghambat dokter dalam mendiagnosis penyakit secara tepat waktu. Hal ini menunjukkan bahwa perang siber tidak hanya mengganggu kelangsungan operasional fasilitas kesehatan, tetapi juga secara langsung mengancam keselamatan pasien.

   Dari sisi hukum, serangan terhadap peralatan medis dapat dikategorikan sebagai pelanggaran terhadap prinsip proporsionalitas dan kemanusiaan dalam Hukum Humaniter Internasional, terlebih jika serangan tersebut disengaja dan menyebabkan kerugian pada warga sipil. Oleh karena itu, diperlukan standar keamanan siber yang ketat untuk semua perangkat medis yang terkoneksi jaringan, serta integrasi aspek keamanan digital ke dalam regulasi dan kebijakan hukum kesehatan internasional.

Analisis Hukum: Pelanggaran Hukum Kesehatan Internasional

1. Pelanggaran Prinsip Netralitas

   Prinsip netralitas dalam Hukum Humaniter Internasional (HHI) mengharuskan agar fasilitas kesehatan dan personel medis tidak menjadi sasaran serangan dalam setiap konflik bersenjata. Prinsip ini didasarkan pada keyakinan bahwa tindakan medis harus bebas dari intervensi militer agar dapat memberikan perawatan yang tidak memihak kepada semua pihak yang membutuhkan. Dengan demikian, serangan siber yang menargetkan fasilitas kesehatan merupakan pelanggaran serius terhadap kewajiban hukum internasional ini. Dalam konteks perang siber Rusia-Ukraina, penargetan sistem digital rumah sakit dan klinik tidak hanya mengancam operasi medis tetapi juga melanggar netralitas fasilitas kesehatan yang seharusnya dilindungi secara ketat oleh Konvensi Jenewa dan protokol tambahannya. Hal ini berdampak pada terganggunya layanan medis dan berpotensi menimbulkan kerugian jiwa, yang melanggar prinsip dasar perlindungan kemanusiaan.
2. Pelanggaran Prinsip Kemanusiaan

   Prinsip kemanusiaan dalam Hukum Humaniter Internasional mengharuskan semua pihak dalam konflik untuk meminimalkan penderitaan manusia dan menjamin akses yang aman dan tidak terganggu ke perawatan medis. Serangan siber yang menghalangi akses pasien ke layanan kesehatan, mematikan sistem informasi rumah sakit, atau menimbulkan gangguan operasional yang membahayakan nyawa pasien merupakan pelanggaran serius terhadap prinsip ini. Misalnya, serangan yang menyebabkan kegagalan ventilator atau alat medis kritis dapat menimbulkan kematian yang seharusnya dapat dicegah. Selain itu, perlindungan terhadap data pasien juga merupakan bagian dari prinsip kemanusiaan karena data tersebut penting untuk memastikan kontinuitas dan kualitas perawatan medis
3. Pelanggaran Prinsip Proporsionalitas

   Prinsip proporsionalitas dalam Hukum Humaniter Internasional mengatur bahwa tindakan militer, termasuk serangan siber, harus seimbang antara keuntungan militer yang diharapkan dan potensi kerugian terhadap warga sipil atau objek sipil, seperti fasilitas kesehatan. Bahkan jika suatu rumah sakit atau fasilitas medis digunakan untuk kepentingan militer oleh salah satu pihak dalam konflik, serangan terhadapnya hanya diperbolehkan apabila keuntungan militer yang diperoleh secara langsung melebihi kerugian sipil yang ditimbulkan. Dalam konteks perang siber, penerapan prinsip ini menjadi semakin kompleks karena dampak serangan digital sering kali

Permasalahan

Tantangan dalam Penegakan Hukum Kesehatan Internasional di Ranah Siber

1. Atribusi

   Salah satu tantangan utama dalam menegakkan hukum kesehatan internasional di ranah siber adalah proses atribusi, yakni mengidentifikasi pelaku serangan siber dengan akurat. Pelaku sering menggunakan berbagai teknik canggih, seperti penyamaran alamat IP, penggunaan server proxy, VPN, dan serangan melalui pihak ketiga, sehingga menyulitkan pelacakan langsung sumber serangan. Kompleksitas ini diperparah oleh kecanggihan teknologi yang memungkinkan serangan dilakukan secara anonim dan lintas batas negara. Ketiadaan identitas yang jelas menyebabkan kesulitan dalam menentukan tanggung jawab hukum dan menuntut pertanggungjawaban pelaku di forum internasional atau nasional. Oleh karena itu, tanpa kemampuan atribusi yang andal, penegakan hukum menjadi tidak efektif dan menghambat perlindungan fasilitas kesehatan dari serangan siber
2. Kepatuhan

   Bahkan jika pelaku diidentifikasi dan yurisdiksi ditetapkan, menegakkan kepatuhan terhadap hukum internasional adalah tantangan karena negara mungkin tidak bersedia menyerahkan warganya atau bekerja sama dalam penyelidikan.
3. Yurisdiksi

Menentukan yurisdiksi atas kejahatan siber adalah kompleks karena serangan dapat berasal dari negara yang berbeda dari tempat kerusakan terjadi. Ini menyulitkan untuk membawa pelaku ke pengadilan.

4. Bukti

   Mengumpulkan dan menyajikan bukti digital di pengadilan adalah tantangan karena bukti dapat dengan mudah diubah atau dihancurkan. Memastikan integritas dan keaslian bukti digital adalah penting untuk penuntutan yang berhasil.

KESIMPULAN

Perang siber Rusia-Ukraina telah menyoroti kerentanan sistem kesehatan terhadap serangan digital yang semakin kompleks dan meluas. Serangan siber yang menargetkan rumah sakit, sistem rekam medis, dan peralatan medis vital telah menyebabkan gangguan layanan kesehatan, pelanggaran data pasien, dan bahkan ancaman langsung terhadap keselamatan jiwa. Situasi ini menuntut perhatian serius dalam kerangka Hukum Kesehatan Internasional dan Hukum Humaniter Internasional (HHI).

Secara hukum, Konvensi Jenewa IV Tahun 1949, khususnya Pasal 18, serta Protokol Tambahan I Tahun 1977, secara tegas memberikan perlindungan khusus terhadap fasilitas dan personel medis selama konflik bersenjata. Fasilitas kesehatan tidak boleh dijadikan target serangan, dan bahkan jika digunakan untuk tujuan militer, prinsip Proporsionalitas, Pencegahan Korban Sipil, dan Netralitas tetap harus dihormati (lihat Pasal 51 dan 57 Protokol Tambahan I).

Namun, konsep hukum ini sebagian besar dirancang untuk konflik konvensional, bukan untuk perang siber yang sering kali tidak menunjukkan pelaku secara langsung (non-attributed), menyeberangi batas negara tanpa pasukan fisik, dan mengandalkan metode yang tidak selalu menghasilkan kerusakan fisik yang langsung terlihat.

Keterbatasan dalam atribusi pelaku serangan, jurisdiksi lintas negara, serta ketidakpastian mengenai penerapan prinsip-prinsip HHI pada serangan digital, menunjukkan adanya kesenjangan antara realitas konflik modern dan perangkat hukum yang ada. Misalnya, Tallinn Manual 2.0 on the International Law Applicable to *"Cyber Operations"* memang memberi panduan interpretatif atas hukum yang berlaku untuk serangan siber, tetapi belum bersifat mengikat secara hukum.

Oleh karena itu, langkah-langkah pembaruan hukum dan kebijakan sangat mendesak, yang meliputi:

1. Penguatan hukum internasional; memperjelas cakupan perlindungan fasilitas kesehatan terhadap serangan digital dalam instrumen hukum internasional yang ada, atau dengan membentuk instrumen baru yang mengatur konflik di ranah siber secara eksplisit.
2. Kerja Sama Internasional; melalui forum seperti WHO, ICRC, dan PBB, negara-negara dapat membentuk mekanisme koordinasi respons terhadap serangan siber lintas batas, pertukaran informasi intelijen, serta proses ekstradisi pelaku.
3. Investasi dalam pelatihan dan teknologi; personel medis, aparat penegak hukum, dan pembuat kebijakan harus memahami risiko dan respons terhadap serangan siber, sementara rumah sakit dan sistem kesehatan harus dilengkapi dengan protokol keamanan digital yang kuat dan adaptif.
4. Perlunya pendekatan multistakeholder; negara, organisasi internasional, sektor swasta (khususnya bidang teknologi), dan masyarakat sipil perlu terlibat dalam menciptakan ekosistem perlindungan siber yang komprehensif untuk sektor kesehatan.
5. Dengan menggabungkan dasar hukum yang jelas dan respons kebijakan yang strategis, kita dapat membangun ketahanan hukum dan teknis terhadap ancaman perang siber dalam sektor kesehatan — memastikan bahwa, bahkan dalam masa konflik, hak atas perawatan medis yang aman dan terlindungi tetap dijunjung tinggi.

REFERENSI

Ahmad Mohee, M. (2023). *Signifikansi perang siber dalam konflik modern Rusia-Ukraina*. Jurnal Ilmu Sosial dan Humaniora, 12(2).

Ibrahim, M. (2019). *Pelanggaran hukum humaniter internasional dalam konflik Rusia-Ukraina*. Novum Law Journal, 6(1).

International Committee of the Red Cross (ICRC), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, hlm. 720–722; serta Trisakti, U., *Pelanggaran Hukum pada Invasi Rusia–Ukraina Ditinjau dari Perspektif Hukum Humaniter Internasional*, Teras Law Review, Vol. 8, No. 2, 2024, hlm. 230–232.

Kshetri, N. (2020). Attribution challenges in cybersecurity: A review. *Journal of Cybersecurity, 6*(1), 22–28. https://doi.org/10.1093/cybsec/tyaa003

Kusuma, R. (2023). *Perlindungan hukum internasional terhadap warga sipil dalam konflik siber Rusia-Ukraina*. Jurnal Dinamika Hukum, 23(4).

Ningsih, Y. (2022). *Memahami perang siber Rusia dan peran badan intelijen negara*. Jurnal IPTEK Kominfo, 16(1). citeturn0search1.

Nye, J. S. (2010). *Cyber power*. Harvard University Press.

Politeknik Siber dan Sandi Negara. (2023). *Perang Rusia-Ukraina: Perspektif siber dan dampaknya terhadap keamanan nasional*. Buku Perspektif Siber, 1.

Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Suharto, M. A. (2024). *Pengaturan tentang cyber warfare dalam hukum humaniter internasional dan analisis pertanggungjawaban hukum terhadap Rusia*. Diponegoro Law Journal, 13(3). citeturn0search2

Suryakusumah, D. (2022). *Analisis pengaruh ancaman cyber war Rusia dan Ukraina terhadap keamanan nasional Indonesia*. Jurnal Pertahanan dan Bela Negara, 12(3).

Susilo, B. (2023). *Antisipasi pengaruh perang Rusia-Ukraina dalam konteks keamanan siber Indonesia*. Lembaga Ketahanan Nasional RI, 26.

Trisakti, U. (2024). *Pelanggaran hukum pada invasi Rusia-Ukraina ditinjau dari perspektif hukum humaniter internasional*. Teras Law Review, 8(2). citeturn0search4.

Universitas Negeri Surabaya. (2020). *Pelanggaran hukum humaniter internasional dalam konflik Rusia-Ukraina*. Novum Law Journal, 5(3).