Media Hukum Indonesia (MHI)
Published by Yayasan Daarul Huda Krueng Mane
https://ojs.daarulhuda.or.id/index.php/MHI/index

June-2025. Vol. 3, No. 2
e-ISSN: 3032-6591
pp 660-665

Analisis Yuridis Tanggung Jawab Negara (State Responsibility) Terhadap Serangan Siber Oleh Aktor Non-Negara Dalam Perspektif Hukum Internasional

(*Legal Analysis of State Responsibility Against Cyber Attacks By Non-State Actors From An International Law Perspective)*

Rifky Justicyo Syahputra[1], Irwan Triadi[2]
Fakultas Hukum Universitas Pembangunan Nasional "Veteran" Jakarta
e-mail : 2310611192@mahasiswa.upnvj.ac.id, irwantriadi1@yahoo.com

Abstract: Era digital telah meningkatkan ketergantungan global pada infrastruktur siber, namun sekaligus membuka kerentanan terhadap serangan siber lintas negara. Fenomena ini menjadi kompleks secara yuridis ketika serangan dilakukan oleh aktor non-negara (*non-state actors*), yang menimbulkan pertanyaan fundamental mengenai akuntabilitas negara dari mana serangan tersebut berasal. Penelitian ini bertujuan untuk menganalisis penerapan prinsip tanggung jawab negara (*state responsibility*) dalam hukum internasional, khususnya mengenai bagaimana tindakan aktor non-negara dapat diatribusikan kepada suatu negara. Selain itu, penelitian ini juga mengidentifikasi tantangan-tantangan yuridis yang fundamental dalam proses pembuktian dan penegakan hukum terhadap negara yang diduga terlibat atau lalai. Dengan menggunakan metode penelitian hukum normatif melalui pendekatan perundang-undangan (*statute approach*) dan studi kasus (*case approach*), artikel ini mengkaji sumber-sumber hukum primer dan sekunder seperti *Articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA), Piagam PBB, serta doktrin yang relevan termasuk Tallinn Manual 2.0. Hasil analisis menunjukkan bahwa standar atribusi berdasarkan 'kendali efektif' (*effective control*) sulit untuk dipenuhi dalam konteks serangan siber yang anonim dan terdesentralisasi. Akibatnya, fokus pertanggungjawaban bergeser pada pelanggaran kewajiban uji tuntas (*due diligence*), di mana sebuah negara dapat dianggap bertanggung jawab jika terbukti lalai dalam mencegah atau menindak aktivitas siber berbahaya dari wilayahnya. Kendati demikian, tantangan signifikan tetap ada dalam hal pembuktian teknis dan keterbatasan mekanisme penegakan hukum internasional yang efektif dan tidak eskalatif.

Abstract *The digital era has increased global dependence on cyber infrastructure, yet it has also created vulnerabilities to transnational cyberattacks. This phenomenon becomes legally complex when attacks are carried out by non-state actors, raising fundamental questions about the accountability of the state from which such attacks originate. This research aims to analyze the application of the principle of state responsibility in international law, particularly concerning how the actions of non-state actors can be attributed to a state. Furthermore, this study identifies the fundamental juridical challenges in the process of evidence-gathering and law enforcement against states suspected of involvement or negligence. Using a normative legal research method with a statute approach and a case study approach, this article examines primary and secondary legal sources such as the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), the UN Charter, and relevant doctrines including the Tallinn Manual 2.0. The findings indicate that the attribution standard based on 'effective control' is difficult to meet in the context of anonymous and decentralized cyberattacks. Consequently, the focus of responsibility shifts to the breach of the due diligence obligation, where a state can be held accountable if proven negligent in preventing or responding to malicious cyber activities from its territory. Nevertheless, significant challenges remain in terms of technical evidence and the limitations of effective, non-escalatory international enforcement mechanisms.*

Article History
Received: June 15, 2025
Revised: June 22, 2025
Published: June 28, 2025

Kata Kunci:
Tanggung Jawab Negara, Serangan Siber, Aktor Non-Negara, Atribusi, *Due Diligence*.

Keywords:
State Responsibility, Cyberattack, Non-State Actors, Attribution, Due Diligence.

https://doi.org/10.5281/zenodo.15766129

PENDAHULUAN

Era digital yang ditandai oleh interkonektivitas global telah menciptakan sebuah paradoks: kemajuan teknologi berjalan seiring dengan meningkatnya kerentanan terhadap ancaman siber. Salah satu ancaman paling signifikan datang dari serangan siber lintas negara yang semakin masif dan

Media Hukum Indonesia (MHI)
Published by Yayasan Daarul Huda Krueng Mane
https://ojs.daarulhuda.or.id/index.php/MHI/index

June-2025. Vol. 3, No. 2
e-ISSN: 3032-6591
pp 660-665

kompleks. Kondisi ini diperumit ketika serangan tersebut tidak lagi dimonopoli oleh negara, melainkan seringkali dilakukan oleh aktor non-negara (*non-state actors*) seperti kelompok peretas, organisasi kriminal, atau proksi yang beroperasi dalam zona abu-abu hukum internasional. Akibatnya, muncul pertanyaan fundamental mengenai bagaimana tanggung jawab negara (*state responsibility*) dapat ditegakkan ketika wilayah atau infrastrukturnya digunakan oleh aktor-aktor tersebut untuk merugikan negara lain.

Dampak dari serangan ini sangat nyata dan meluas. Serangan siber mampu mengganggu layanan esensial seperti kesehatan dan pendidikan, menyebabkan kerugian ekonomi yang signifikan bagi negara dan warganya.[1] Kompleksitas hukumnya semakin dalam karena norma-norma yang ada, seperti Hukum Humaniter Internasional (IHL) yang berupaya membatasi dampak konflik bersenjata, menghadapi tantangan adaptasi dalam konteks perang siber yang seringkali nirbatas dan melibatkan kombatan yang tidak jelas.[2]

Tantangan fundamental dalam menegakkan akuntabilitas terletak pada masalah atribusi, yaitu proses menghubungkan sebuah serangan siber kepada pelaku spesifik, dan yang lebih sulit lagi, kepada negara sponsornya. Upaya untuk menindak pelaku melalui metode publik seperti "menamakan dan memalukan" (*naming and shaming*) terbukti seringkali tidak efektif tanpa adanya bukti teknis dan hukum yang kuat, sehingga kredibilitas klaim negara korban sering dipertanyakan.[3] Masalah atribusi ini secara langsung berimplikasi pada kedaulatan negara dan legitimasi tindakan balasan apa pun yang mungkin diambil, terutama ketika data dan identitas pelaku sulit dilacak.[4]

Dilema ini memuncak ketika negara korban berusaha menggunakan haknya untuk membela diri (*self-defense*). Meskipun hukum internasional mengakui hak ini, merespons serangan siber dari aktor non-negara dengan tindakan balasan dapat memicu risiko eskalasi konflik yang berbahaya.[5] Tanpa parameter hukum yang jelas mengenai kapan dan bagaimana sebuah negara dapat secara sah membalas, tindakan defensif sekalipun dapat disalahartikan sebagai agresi.

Berdasarkan paparan di atas, terlihat adanya kekosongan dan ketidakpastian hukum yang serius. Di satu sisi, dampak serangan siber oleh aktor non-negara sangat merusak. Di sisi lain, kerangka hukum internasional yang ada saat ini menghadapi kesulitan dalam hal atribusi, pembuktian, dan penegakan tanggung jawab negara. Oleh karena itu, penelitian ini menjadi krusial untuk menganalisis secara mendalam bagaimana prinsip-prinsip fundamental tanggung jawab negara, khususnya prinsip atribusi dan kewajiban uji tuntas (*due diligence*), dapat diterapkan secara efektif dalam konteks unik serangan siber oleh aktor non-negara.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kepustakaan (*library research*) dengan pendekatan yuridis normatif. Metode penelitian kepustakaan merupakan teknik yang dilakukan melalui pengumpulan data dan informasi dari berbagai literatur, seperti perjanjian internasional, jurnal hukum, artikel, serta dokumen-dokumen hukum internasional yang relevan. Pendekatan yuridis normatif digunakan untuk menganalisis norma, asas, dan prinsip hukum internasional yang mengatur tanggung jawab negara, khususnya dalam konteks keamanan siber.

Pendekatan yuridis normatif memungkinkan peneliti untuk melakukan kajian yang mendalam terhadap teks-teks hukum, Dungan tujuan memahami dan mengevaluasi bagaimana prinsip atribusi (*attribution*) dan kewajiban uji tuntas (*due diligence*) diterapkan pada serangan siber oleh aktor non-negara. Penelitian ini mengandalkan sumber data sekunder, yang terdiri dari bahan hukum primer,

[1] Mazaraki, N. and Goncharova, Y. (2022). Cyber dimension of hybrid wars: escaping a ‘grey zone’ of international law to adress economic damages. Baltic Journal of Economic Studies, 8(2), 115-120. https://doi.org/10.30525/2256-0742/2022-8-2-115-120
[2] Goyal, A. (2023). The role of international human law in armed conflicts involving non- state actors an analytical study. pne, 55(01). https://doi.org/10.48047/pne.2018.55.1.39
[3] Aravindakshan, S. (2020). Cyberattacks: a look at evidentiary thresholds in international law. Indian Journal of International Law, 59(1-4), 285-299. https://doi.org/10.1007/s40901-020-00113-0
[4] Gunatileka, S. (2024). “big data breaches”, sovereignty of states and the challenges in attribution. University of Colombo Review, 5(1), 104-129. https://doi.org/10.4038/ucr.v5i1.99
[5] Escobar, T. (2023). Self-defense strategies against cyber- attacks by non-state actors. Revista De Relaciones Internacionales Estrategia Y Seguridad, 18(2), 61-72. https://doi.org/10.18359/ries.6639

June-2025. Vol. 3, No. 2
e-ISSN: 3032-6591
pp 660-665

seperti hukum kebiasaan internasional dan putusan pengadilan internasional, serta bahan hukum sekunder, seperti doktrin para ahli, artikel jurnal, dan buku teks.

Dalam proses pengumpulan data, penelitian ini mengkaji *Articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA) 2001, Piagam PBB, serta putusan-putusan penting dari Mahkamah Internasional (ICJ) seperti kasus *Nicaragua*. Data-data ini kemudian dianalisis dengan menggunakan teknik interpretasi hukum (*legal interpretation*) untuk mendapatkan pemahaman yang komprehensif mengenai penerapan prinsip tanggung jawab negara dalam menghadapi tantangan serangan siber oleh aktor non-negara di era digital.

HASIL DAN PEMBAHASAN

Parameter hukum internasional, khususnya melalui prinsip atribusi (*attribution*) dan kewajiban uji tuntas (*due diligence*), diterapkan untuk menentukan tanggung jawab suatu negara atas serangan siber yang dilancarkan oleh aktor non-negara dari dalam wilayahnya

Untuk menentukan tanggung jawab negara (*state responsibility*) atas serangan siber yang dilancarkan oleh aktor non-negara, hukum internasional menyediakan kerangka yuridis yang bertumpu pada dua pilar utama: prinsip atribusi (*attribution*) dan kewajiban uji tuntas (*due diligence*). Kedua pilar ini bekerja secara komplementer untuk menilai apakah suatu negara dapat dimintai pertanggungjawaban, baik karena keterlibatan langsung maupun karena kelalaian yang berakibat fatal.

Pilar pertama, prinsip atribusi, merupakan standar tertinggi dalam penentuan tanggung jawab. Prinsip ini berupaya menjawab pertanyaan fundamental: apakah tindakan kelompok peretas dapat secara hukum dianggap sebagai "tindakan negara" itu sendiri? Standar pembuktian untuk ini sangatlah ketat. Berdasarkan hukum kebiasaan internasional yang dikodifikasikan dalam *Articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA) dan preseden Mahkamah Internasional dalam kasus *Nicaragua v. Amerika Serikat*, sebuah tindakan hanya dapat diatribusikan jika aktor non-negara tersebut bertindak atas "instruksi, arahan, atau di bawah kendali efektif" negara.[6][7] Namun, memenuhi ambang batas "kendali efektif" di dunia siber yang anonim nyaris mustahil. Sifat serangan yang terdesentralisasi dan penggunaan teknologi untuk menyamarkan jejak digital memberikan ruang bagi negara untuk melakukan penyangkalan yang masuk akal (*plausible deniability*), sehingga menantang interpretasi tradisional hukum internasional dalam dilema keamanan siber modern.[8]

Sulitnya memenuhi standar atribusi yang ketat tersebut mengarahkan fokus analisis hukum pada pilar kedua yang lebih praktis: kewajiban uji tuntas (*due diligence*). Prinsip ini tidak lagi menuntut bukti "kendali" negara atas peretas, melainkan berfokus pada apakah negara telah lalai memenuhi kewajibannya untuk mengambil semua langkah yang wajar (*reasonable measures*) untuk mencegah wilayahnya digunakan sebagai basis serangan yang merugikan negara lain. Kewajiban ini bersifat proaktif dan reaktif, serta menjadi tolok ukur perilaku negara yang bertanggung jawab di era digital.

Pemenuhan kewajiban *due diligence* dalam konteks siber dapat diukur melalui beberapa tindakan konkret. Pertama, negara harus memiliki kerangka legislatif nasional yang memadai untuk mengkriminalisasi aktivitas siber berbahaya, di mana pembaruan hukum yang adaptif menjadi kunci.[9] Kedua, negara harus menunjukkan kapasitas penegakan hukum untuk menginvestigasi dan menindak pelaku di wilayahnya. Ketiga, negara wajib menunjukkan itikad baik untuk bekerja sama secara internasional, baik melalui pertukaran informasi maupun bantuan investigasi, sebagaimana diwujudkan dalam kerja sama regional seperti di ASEAN untuk memperkuat ketahanan siber bersama.[10] Keempat,

[6] Ilmi, A. (2020). Legal opinion : nicaragua v. united states of america. Jurnal Hukum Lex Generalis, 1(1), 1-12. https://doi.org/10.56370/jhlg.v1i1.189
[7] Wathan, B. and Putri, I. (2024). Analisa hukum kebiasaan dalam kasus militer dan paramiliter nikaragua v. amerika serikat. Innovative Journal of Social Science Research, 4(3), 837-846. https://doi.org/10.31004/innovative.v4i3.10389
[8] Sukmawan, D. and Setyawan, D. (2023). Hacker, fear, and harm: data breaches and national security. Jurnal Global & Strategis, 17(1), 153-182. https://doi.org/10.20473/jgs.17.1.2023.153-182
[9] Ramayanti, H. and Lubis, A. (2023). Peran hukum dalam mengatasi serangan cyber yang mengancam keamanan nasional. Jurnal Hukum Dan Ham Wara Sains, 2(09). https://doi.org/10.58812/jhhws.v2i09.672
[10] Putri, K. (2021). Kerja sama indonesia dengan asean mengenai cyber security dan cyber resilience dalam mengatasi cyber crime. Jurnal Hukum Lex Generalis, 2(7), 542-554. https://doi.org/10.56370/jhlg.v2i7.90

June-2025. Vol. 3, No. 2
e-ISSN: 3032-6591
pp 660-665

negara juga diharapkan menerapkan langkah-langkah teknis preventif, seperti penggunaan *Intrusion Detection Systems* (IDS), sebagai bukti upaya melindungi infrastruktur dan mencegah serangan.[11]

Dengan demikian, negara yang secara sadar membiarkan kelompok peretas beroperasi bebas, menolak bekerja sama, atau secara nyata gagal melindungi infrastruktur pentingnya, dapat dianggap telah melanggar kewajiban uji tuntasnya dan karenanya bertanggung jawab secara internasional.[12] Pada akhirnya, meskipun atribusi menjadi bukti keterlibatan langsung yang paling dicari, kewajiban *due diligence* telah menjadi standar de facto yang lebih fungsional dan krusial untuk menilai tanggung jawab negara dalam menghadapi ancaman siber yang kompleks dan terus berkembang.

Tantangan yuridis fundamental dalam proses pembuktian keterlibatan negara dan penerapan mekanisme penegakan hukum (seperti *countermeasures*) terhadap negara yang dinilai gagal memenuhi kewajibannya

Setelah menguraikan parameter hukum untuk tanggung jawab negara, analisis selanjutnya berfokus pada tantangan-tantangan yuridis fundamental yang muncul dalam praktik. Tantangan pertama dan paling fundamental dalam penegakan hukum siber adalah proses pembuktian. Di dunia siber, serangan seringkali dilancarkan secara anonim melalui jaringan yang terenkripsi dan terdesentralisasi, membuatnya sangat sulit untuk mengidentifikasi pelaku secara definitif. Kejahatan siber seringkali tidak meninggalkan jejak yang jelas, sehingga atribusi serangan kepada aktor non-negara tertentu (apalagi mengaitkannya dengan sponsor negara) menjadi penghalang utama. Tanpa bukti yang kuat, setiap upaya untuk menuntut pertanggungjawaban akan runtuh di awal. Kondisi ini diperumit oleh prinsip pembelaan diri negara yang dituduh, yaitu melalui pemenuhan kewajiban uji tuntas (*due diligence*). Sebuah negara dapat berargumen bahwa mereka tidak bertanggung jawab karena telah mengambil semua langkah yang wajar untuk mencegah serangan tersebut, menciptakan "medan pertempuran" yuridis yang kompleks di mana pembuktian timbal-balik seringkali tidak meyakinkan.[13]

Namun, seandainya pun tantangan pembuktian yang berat ini dapat diatasi dan keterlibatan atau kelalaian negara berhasil diidentifikasi, negara korban dihadapkan pada serangkaian dilema yuridis baru dalam tahap penegakan hukum. Mekanisme utama yang tersedia adalah tindakan balasan (*countermeasures*), yaitu tindakan yang diizinkan sebagai respons terhadap pelanggaran hukum internasional oleh negara lain. Akan tetapi, penerapannya di ranah siber penuh dengan ketidakpastian hukum dan risiko. Kerangka hukum tradisional mengenai konflik bersenjata tidak dapat diterapkan secara langsung, menciptakan kekaburan aturan main di dunia siber.[14]

Salah satu dilema terbesar adalah memastikan tindakan balasan bersifat proporsional. Hukum internasional mensyaratkan bahwa respons tidak boleh menyebabkan kerugian yang lebih besar daripada serangan awalnya. Dalam konteks serangan terhadap infrastruktur kritis, tindakan balasan yang sepadan bisa jadi memiliki dampak kemanusiaan yang dahsyat dan tidak terduga terhadap warga sipil, menciptakan dilema antara menegakkan hukum dan melindungi hak asasi manusia.[15] Ketidakjelasan mengenai batasan proporsionalitas ini terbukti bahkan dalam konflik besar; dalam kasus invasi Rusia ke Ukraina, tidak ada konsensus internasional yang jelas mengenai jenis tindakan balasan siber yang dapat diterima.[16]

Pada akhirnya, penegakan hukum internasional tidak pernah lepas dari realitas politik dan keterbatasan kapasitas. Negara berkembang mungkin tidak memiliki sumber daya untuk membuktikan

[11] Maulani, I., Putra, D., & Komarudin, K. (2023). Sistem deteksi intrusi cerdas: studi perbandingan algoritma pembelajaran mesin untuk keamanan siber. Jurnal Sosial Teknologi, 3(11), 918-923. https://doi.org/10.59188/jurnalsostech.v3i11.987
[12] Arafat, M. and Wirasto, A. (2024). Kebijakan kriminal dalam penanganan siber di era digital: studi kasus di indonesia. Equality-JLJ, 1(2), 220-241. https://doi.org/10.69836/equality-jlj.v1i2.170
[13] Meilinda, D. (2022). Implementasi due deligence notaris sebelum dan sesudah perusahaan badan hukum pt listing di pasar modal abstrak. JPJ, 3(1). https://doi.org/10.57084/jpj.v3i1.852
[14] Sarjito, A. (2023). Memikirkan kembali kebijakan pertahanan di era peperangan siber. Jurnal Publisitas, 10(1), 76-91. https://doi.org/10.37858/publisitas.v10i1.330
[15] Imasfy, M. (2025). Kajian hukum humaniter internasional mengenai perang siber dalam kaitannya dengan serangan infrastruktur kritis. Jurnal Sosial Dan Sains, 5(5), 1386-1399. https://doi.org/10.59188/jurnalsosains.v5i5.32190
[16] Sudiq, R. and Yustitianingtyas, L. (2022). Intervensi rusia terhadap ukraina pada tahun 2022 sebagai pelanggaran berat ham. Jurnal Pendidikan Kewarganegaraan Undiksha, 10(3), 101-117. https://doi.org/10.23887/jpku.v10i3.51278

June-2025. Vol. 3, No. 2
e-ISSN: 3032-6591
pp 660-665

kasusnya atau bahkan untuk memenuhi kewajiban *due diligence*-nya secara penuh.[17] Di sisi lain, negara-negara besar seringkali lebih memilih jalur diplomasi atau negosiasi daripada mengambil risiko eskalasi melalui tindakan balasan siber. Faktor geopolitik seringkali lebih berpengaruh daripada pertimbangan hukum murni. Oleh karena itu, untuk bergerak maju, penegakan hukum yang efektif membutuhkan kerja sama multi-pihak yang melibatkan sektor publik dan swasta untuk membangun mekanisme yang lebih adaptif dan diterima secara global guna menghadapi ancaman siber yang terus berkembang.[18]

SIMPULAN

Berdasarkan analisis yang telah dilakukan, dapat ditarik kesimpulan mengenai kompleksitas yuridis tanggung jawab negara atas serangan siber oleh aktor non-negara. Hukum internasional menyediakan parameter penentuan tanggung jawab melalui dua pilar utama. Pilar pertama adalah prinsip atribusi, yang memiliki ambang batas pembuktian sangat tinggi karena mensyaratkan adanya "kendali efektif" negara atas pelaku, suatu hal yang sulit dipenuhi dalam praktiknya di dunia siber. Akibatnya, pilar kedua, yaitu kewajiban uji tuntas (*due diligence*), menjadi lebih relevan dan krusial. Melalui pilar ini, tanggung jawab negara dinilai berdasarkan ada atau tidaknya kelalaian untuk mengambil langkah-langkah yang wajar dalam mencegah dan merespons serangan dari wilayahnya. Selain itu, penelitian ini juga menyimpulkan bahwa terdapat tantangan fundamental dalam tataran praktik. Tantangan tersebut mencakup kesulitan dalam pembuktian teknis yang bersifat anonim, kompleksitas menilai pemenuhan *due diligence* suatu negara, serta dilema dalam penerapan mekanisme penegakan hukum seperti tindakan balasan (*countermeasures*) yang dibatasi oleh syarat proporsionalitas dan realitas politik global.

SARAN

Bertolak dari kesimpulan tersebut, beberapa saran diajukan untuk mengatasi tantangan yang ada. Di tingkat global, komunitas internasional perlu melanjutkan upaya untuk memperjelas norma perilaku negara yang bertanggung jawab di ruang siber, terutama dengan merumuskan secara lebih detail tindakan-tindakan spesifik yang merupakan bagian dari kewajiban *due diligence*. Di tingkat nasional, khususnya bagi Indonesia, penguatan kapasitas domestik menjadi sangat penting. Hal ini dapat dilakukan dengan terus memperbarui kerangka hukum siber nasional serta meningkatkan kapabilitas teknis dan sumber daya manusia lembaga terkait seperti BSSN. Upaya domestik ini harus diimbangi dengan peningkatan kerja sama internasional dan regional, misalnya melalui forum ASEAN, untuk memfasilitasi investigasi bersama dan membangun respons yang terkoordinasi. Lebih jauh lagi, pendekatan yang komprehensif menuntut adanya model kerja sama multi-pihak yang efektif, dengan melibatkan sektor swasta yang memiliki peran vital dalam ekosistem siber untuk pencegahan dan penanggulangan ancaman secara kolaboratif.

REFERENSI

Anggara, A. and Dinata, M. (2023). Hacker bjorka: pihak yang berperan dalam mencegah kebocoran data. *Jurnal Hukum Magnum Opus, 6*(1). https://doi.org/10.30996/jhmo.v6i1.8293

Arafat, M. and Wirasto, A. (2024). Kebijakan kriminal dalam penanganan siber di era digital: studi kasus di indonesia. *Equality-JLJ, 1*(2), 220-241. https://doi.org/10.69836/equality-jlj.v1i2.170

Aravindakshan, S. (2020). Cyberattacks: a look at evidentiary thresholds in international law. *Indian Journal of International Law, 59*(1-4), 285-299. https://doi.org/10.1007/s40901-020-00113-0

Escobar, T. (2023). Self-defense strategies against cyber- attacks by non-state actors. *Revista De Relaciones Internacionales Estrategia Y Seguridad, 18*(2), 61-72. https://doi.org/10.18359/ries.6639

[17] Rachman, A. and Hastri, E. (2021). Implikasi prinsip right of external self determination terhadap kedaulatan negara induk sebagai subjek hukum internasional. Jurnal Jendela Hukum, 8(2), 47-63. https://doi.org/10.24929/fh.v8i2.1578

[18] Anggara, A. and Dinata, M. (2023). Hacker bjorka: pihak yang berperan dalam mencegah kebocoran data. Jurnal Hukum Magnum Opus, 6(1). https://doi.org/10.30996/jhmo.v6i1.8293

June-2025. Vol. 3, No. 2
e-ISSN: 3032-6591
pp 660-665

Goyal, A. (2023). The role of international human law in armed conflicts involving non- state actors an analytical study. *pne, 55*(01). https://doi.org/10.48047/pne.2018.55.1.39

Gunatileka, S. (2024). "big data breaches", sovereignty of states and the challenges in attribution. *University of Colombo Review, 5*(1), 104-129. https://doi.org/10.4038/ucr.v5i1.99

Ilmi, A. (2020). Legal opinion : nicaragua v. united states of america. *Jurnal Hukum Lex Generalis, 1*(1), 1-12. https://doi.org/10.56370/jhlg.v1i1.189

Imasfy, M. (2025). Kajian hukum humaniter internasional mengenai perang siber dalam kaitannya dengan serangan infrastruktur kritis. *Jurnal Sosial Dan Sains, 5*(5), 1386-1399. https://doi.org/10.59188/jurnalsosains.v5i5.32190

Maulani, I., Putra, D., & Komarudin, K. (2023). Sistem deteksi intrusi cerdas: studi perbandingan algoritma pembelajaran mesin untuk keamanan siber. *Jurnal Sosial Teknologi, 3*(11), 918-923. https://doi.org/10.59188/jurnalsostech.v3i11.987

Mazaraki, N. and Goncharova, Y. (2022). Cyber dimension of hybrid wars: escaping a 'grey zone' of international law to adress economic damages. *Baltic Journal of Economic Studies, 8*(2), 115-120. https://doi.org/10.30525/2256-0742/2022-8-2-115-120

Meilinda, D. (2022). Implementasi due deligence notaris sebelum dan sesudah perusahaan badan hukum pt listing di pasar modal abstrak. *JPJ, 3*(1). https://doi.org/10.57084/jpj.v3i1.852

Putri, K. (2021). Kerja sama indonesia dengan asean mengenai cyber security dan cyber resilience dalam mengatasi cyber crime. *Jurnal Hukum Lex Generalis, 2*(7), 542-554. https://doi.org/10.56370/jhlg.v2i7.90

Rachman, A. and Hastri, E. (2021). Implikasi prinsip right of external self determination terhadap kedaulatan negara induk sebagai subjek hukum internasional. *Jurnal Jendela Hukum, 8*(2), 47-63. https://doi.org/10.24929/fh.v8i2.1578

Ramayanti, H. and Lubis, A. (2023). Peran hukum dalam mengatasi serangan cyber yang mengancam keamanan nasional. *Jurnal Hukum Dan Ham Wara Sains, 2*(09). https://doi.org/10.58812/jhhws.v2i09.672

Sarjito, A. (2023). Memikirkan kembali kebijakan pertahanan di era peperangan siber. *Jurnal Publisitas, 10*(1), 76-91. https://doi.org/10.37858/publisitas.v10i1.330

Sudiq, R. and Yustitianingtyas, L. (2022). Intervensi rusia terhadap ukraina pada tahun 2022 sebagai pelanggaran berat ham. *Jurnal Pendidikan Kewarganegaraan Undiksha, 10*(3), 101-117. https://doi.org/10.23887/jpku.v10i3.51278

Sukmawan, D. and Setyawan, D. (2023). Hacker, fear, and harm: data breaches and national security. *Jurnal Global & Strategis, 17*(1), 153-182. https://doi.org/10.20473/jgs.17.1.2023.153-182

Wathan, B. and Putri, I. (2024). Analisa hukum kebiasaan dalam kasus militer dan paramiliter nikaragua v. amerika serikat. *Innovative Journal of Social Science Research, 4*(3), 837-846. https://doi.org/10.31004/innovative.v4i3.10389