JURNAL MEDIA AKADEMIK (JMA)
Vol.3, No.12 Desember 2025
e-ISSN: 3031-5220; DOI: 10.62281, Hal XX-XX
PT. Media Akademik Publisher
AHU-084213.AH.01.30.Tahun 2023

PENERAPAN PRINSIP PEMBEDAAN DAN PROPORSIONALITAS DALAM PERANG SIBER: STUDI KASUS KONFLIK BERSENJATA RUSIA–UKRAINA

Oleh:

Michelle Golda Meir[1]
I Made Budi Arsika[2]

Universitas Udayana
Alamat: JL. Pulau Bali No. 1, Dauh Puri Klod, Kec. Denpasar Barat, Kota Denpasar, Bali (80114).
Korespondensi Penulis: m.goldameir03@gmail.com, budi_arsika@unud.ac.id.

Abstract*. The development of cyber warfare as a modern domain of warfare presents significant challenges to the existing framework of International Humanitarian Law (IHL). This research aims to analyze the challenges in applying fundamental IHL principles specifically distinction and proportionality. Within the context of cyber operations during the Russia–Ukraine armed conflict. Employing a normative juridical research method, this study utilizes a statute approach, a conceptual approach, and a case study approach. Key findings indicate that the unique characteristics of cyber warfare, such as the dual-use nature of infrastructure and the cascading effects of attacks, fundamentally blur the lines between military objectives and civilian objects. This creates substantial difficulties in effectively implementing the principle of distinction. Furthermore, proportionality calculations become highly complex due to the challenges of quantifying non-physical damage and foreseeing excessive incidental harm to the civilian population. This study concludes that while IHL remains applicable, an urgent implementation gap exists. Clarification and strengthening of the IHL framework are required to ensure its relevance and capacity to provide effective protection for civilians in the digital warfare era.*

Received November 08, 2025; Revised November 18, 2025; December 09, 2025
*Corresponding author: *m.goldameir03@gmail.com*

PENERAPAN PRINSIP PEMBEDAAN DAN PROPORSIONALITAS DALAM PERANG SIBER: STUDI KASUS KONFLIK BERSENJATA RUSIA–UKRAINA

Keywords: *Cyber Warfare, Principle of Distinction, Principle of Proportionality, Russia–Ukraine Conflict.*

Abstrak. Perkembangan perang siber sebagai domain peperangan modern menghadirkan tantangan signifikan bagi kerangka Hukum Humaniter Internasional (HHI) yang ada. Penelitian ini bertujuan untuk menganalisis tantangan penerapan prinsip-prinsip fundamental HHI, khususnya prinsip pembedaan dan proporsionalitas. Dalam konteks operasi siber pada konflik bersenjata Rusia–Ukraina. Dengan menggunakan metode penelitian hukum normatif (yuridis normatif), penelitian ini menerapkan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan studi kasus. Temuan utama menunjukkan bahwa karakteristik unik perang siber, seperti sifat infrastruktur berfungsi ganda dan efek serangan yang berjenjang, secara fundamental mengaburkan batasan antara objek militer dan objek sipil. Hal ini menyebabkan kesulitan substansial dalam mengimplementasikan prinsip pembedaan secara efektif. Selain itu, kalkulasi proporsionalitas menjadi sangat kompleks karena sulitnya mengukur kerusakan non-fisik dan memprediksi dampak insidentil yang berlebihan terhadap penduduk sipil. Penelitian ini menyimpulkan bahwa meskipun HHI tetap berlaku, terdapat kesenjangan implementasi yang mendesak. Diperlukan klarifikasi dan penguatan kerangka hukum HHI agar tetap relevan dan mampu memberikan perlindungan efektif bagi warga sipil di era peperangan digital.

Kata Kunci: Perang Siber, Prinsip Pembedaan, Prinsip Proporsionalitas, Konflik Rusia–Ukraina.

LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah secara fundamental mengubah lanskap konflik global, melahirkan domain peperangan kelima setelah darat, laut, udara, dan luar angkasa: ruang siber (*cyberspace*).[1] Era digitalisasi telah mengintegrasikan infrastruktur siber ke dalam setiap aspek kehidupan masyarakat modern, mulai dari sistem perbankan, energi, kesehatan, hingga pemerintahan dan

[1] NATO, "Cyber defence," diperbarui 30 Juli 2024.

pertahanan militer.[2] Ketergantungan yang mendalam ini, di satu sisi, mendorong kemajuan peradaban, akan tetapi di sisi lain, menciptakan kerentanan inheren yang dieksploitasi dalam konflik bersenjata. Perang siber (*cyber warfare*), yang didefinisikan sebagai tindakan yang dilakukan oleh suatu negara-bangsa untuk menembus jaringan komputer atau sistem informasi negara lain dengan tujuan menyebabkan kerusakan atau gangguan,[3] telah berevolusi dari konsep teoretis menjadi komponen integral dalam doktrin militer modern.

Hubungan antara teknologi informasi dan konflik bersenjata internasional[4] melahirkan tantangan yuridis yang signifikan bagi kerangka hukum yang ada, terutama Hukum Humaniter Internasional (HHI).[5] HHI, yang terkodifikasi utamanya dalam Konvensi Jenewa 1949 dan Protokol-Protokol Tambahannya, dirancang untuk mengatur peperangan kinetik yang dicirikan oleh kekerasan fisik, kehancuran yang terlihat, dan batas geografis yang jelas.[6] Sebaliknya, serangan siber memiliki karakteristik unik: bersifat nirbatas (*borderless*),[7] sering kali anonim atau sulit diatribusikan (*problem of attribution*),[8] dan mampu menyebabkan dampak masif yang bersifat non-destruktif secara fisik namun melumpuhkan fungsi vital suatu negara. Sifat ganda (*dual-use*) dari banyak infrastruktur siber—yang melayani kebutuhan sipil dan militer secara bersamaan—semakin mengaburkan batas-batas yang menjadi fondasi utama HHI.[9] Konsekuensinya, penerapan prinsip-prinsip fundamental HHI dalam konteks siber menjadi sebuah tantangan konseptual dan praktis yang mendesak.

Konflik bersenjata antara Federasi Rusia dan Ukraina, yang eskalasinya terjadi sejak Februari 2022, menjadi kasus paling relevan dan komprehensif mengenai integrasi

---

[2] H. Riggs, S. Tufail, I. Parvez, M. Tariq, M. A. Khan, A. Amir, K. V. Vuda, dan A. I. Sarwat, "Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure," *Sensors*, 23, No. 4060, (2023).

[3] Michael N. Schmitt, "Cyber Operations and the Jus in Bello: The Tallinn Manual," *Loyola University Chicago International Law Review* 9, No. 2 (2012): hlm. 99.

[4] Herbert Lin, *"Cyber Conflict and International Humanitarian Law," International Review of the Red Cross* 94, No. 886 (2013): 515–531.

[5] Yahli Shereshevsky, "International Humanitarian Law-Making and New Military Technologies," *International Review of the Red Cross*, 104, Nos. 920–921 (2022): 273–302.

[6] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, 3rd ed. (Cambridge: Cambridge University Press, 2016), hlm. 15–17.

[7] Chen, S., Hao, M., Ding, F. et al. "Exploring the global geography of cybercrime and its driving forces." *Humanit Soc Sci Commun* 10, 71 (2023).

[8] L. Finlay & C. Payne, "The Attribution Problem and Cyber Armed Attacks," *American Journal of International Law*, 113, (2019): 203–204.

[9] Oona A. Hathaway, Azmat Khan & Mara R. Revkin, *"The Dangerous Rise of "Dual-Use" Objects in War," Yale L.J.* 134, no. 8 (2025).

operasi siber dalam peperangan hibrida (*hybrid warfare*).[10] Konflik ini seolah menjadi laboratorium nyata di mana serangan siber dilancarkan secara intensif dan terkoordinasi dengan operasi militer di lapangan. Jauh sebelum invasi militer konvensional, Ukraina telah menjadi target serangan siber canggih yang diduga kuat didalangi oleh aktor negara. Serangan terhadap jaringan listrik Ukraina pada tahun 2015 dan 2016 serta serangan *malware* NotPetya pada tahun 2017 yang melumpuhkan sebagian besar infrastruktur kritis Ukraina menjadi preseden penting.[11] Serangan yang menyamar sebagai *ransomware* tersebut sejatinya adalah *wiper* yang dirancang untuk menghancurkan data, dengan cepat menyebar ke luar Ukraina dan menyebabkan kerugian ekonomi global hingga miliaran dolar, menunjukkan potensi dampak lintas batas dan tak pandang bulu dari senjata siber.

Sejak invasi 2022, spektrum serangan siber semakin intensif dan terkoordinasi dengan operasi militer di lapangan. Salah satu contoh paling signifikan adalah serangan terhadap jaringan satelit Viasat KA-SAT pada 24 Februari 2022, tepat satu jam sebelum invasi dimulai. Serangan ini tidak hanya mengganggu komunikasi militer Ukraina, tetapi juga berdampak pada puluhan ribu pengguna sipil di seluruh Eropa, termasuk menonaktifkan sistem pemantauan turbin angin di Jerman.[12] Selain itu, serangan *Distributed Denial of Service* (DDoS) secara masif menargetkan situs web pemerintah dan perbankan Ukraina, sementara *malware* penghapus data (*wiper*) seperti WhisperGate dan AcidRain dikerahkan untuk merusak sistem komputer pemerintah dan perusahaan.[13] Serangan-serangan tersebut secara nyata menargetkan infrastruktur yang memiliki fungsi sipil dan militer, sehingga menimbulkan pertanyaan krusial mengenai kepatuhan terhadap pilar-pilar utama HHI.

Di tengah kompleksitas perang siber ini, dua prinsip kardinal dalam HHI menjadi diuji: prinsip pembedaan (*distinction*) dan proporsionalitas (*proportionality*). Prinsip pembedaan, sebagaimana diatur dalam Pasal 48 Protokol Tambahan I 1977, mewajibkan

[10] Herbert Lin, *"Russian Cyber Operations in the Invasion of Ukraine," The Cyber Defense Review* 7, No. 4 (2022): 31–46.
[11] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, (22 Agustus 2018).
[12] Council of the European Union, "Declaration by the High Representative on behalf of the European Union on malicious cyber activity conducted by the Russian Federation against Ukraine," *Press Release*, (10 Mei 2022).
[13] Microsoft Threat Intelligence Center, "Destructive 'wiper' malware targeting Ukrainian organizations," *Microsoft Blog*, (24 Februari 2022).

pihak yang bertikai untuk setiap saat membedakan antara penduduk sipil dan kombatan serta antara objek sipil dan sasaran militer.[14] Dalam domain siber, di mana infrastruktur kritis seperti jaringan listrik dan komunikasi bersifat *dual-use*, pemisahan ini menjadi sangat sulit. Serangan terhadap sebuah pusat data militer dapat secara bersamaan melumpuhkan layanan esensial bagi jutaan warga sipil. Sementara itu, prinsip proporsionalitas, yang diatur dalam Pasal 51(5)(b) dan Pasal 57 Protokol Tambahan I dan Aturan 14 Hukum Humaniter Internasional Kebiasaan, melarang serangan yang dapat diperkirakan menyebabkan kerusakan sipil yang bersifat eksesif (*excessive*) apabila dibandingkan dengan keuntungan militer konkrit yang diharapkan.[15] Tantangan utamanya tentu mengenai bagaimana mengukur "kerusakan sipil" dalam konteks siber. Efek berjenjang (*cascading effects*) dari sebuah serangan siber sangat sulit diprediksi *ex ante*, sehingga membuat kalkulasi proporsionalitas menjadi hampir mustahil untuk dilakukan secara akurat dan sah.

Atas dasar itulah, kondisi tersebut menegaskan adanya urgensi akademis dan praktis untuk mengkaji persoalan ini secara mendalam. Konflik Rusia–Ukraina memberikan referensi actual mengenai bagaimana suatu serangan siber dilancarkan, yang kemudian menggiring komunitas internasional untuk menghadapi ambiguitas hukum yang selama ini lebih banyak dibahas secara teoretis. Meskipun telah ada upaya akademis seperti *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, dokumen ini bersifat non-mengikat dan belum mencapai konsensus global.[16]

Berlatar dari situasi tersebut, artikel ini hendak menganalisis tantangan-tantangan dalam implementasi prinsip pembedaan dan proporsionalitas terhadap jenis-jenis serangan siber spesifik yang terjadi dalam konflik Rusia–Ukraina. Kajian ini memiliki relevansi akademik untuk memperkaya literatur HHI dan studi keamanan siber, serta relevansi praktis untuk memberikan panduan bagi negara dan aktor militer dalam merumuskan aturan pelibatan (*rules of engagement*) yang sah, demi memastikan perlindungan terhadap penduduk sipil di tengah evolusi cara dan metode peperangan (*means and methods of warfare*) di era modern.

---

[14] Protokol Tambahan pada Konvensi Jenewa 12 Agustus 1949, dan yang berhubungan dengan Perlindungan Korban-korban Pertikaian Bersenjata Internasional (Protokol I), 8 Juni 1977, 1125 U.N.T.S. 3, Pasal 48.

[15] *Ibid*., Pasal 51(5)(b) dan Pasal 57(2)(a)(iii).

[16] Michael N. Schmitt (gen. ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, (Cambridge University Press, 2017).

KAJIAN TEORITIS

Prinsip Fundamental dalam Hukum Humaniter Internasional

Dalam HHI, *jus in bello* (hukum dalam perang) merupakan seperangkat aturan yang bertujuan untuk membatasi dampak dari konflik bersenjata atas dasar kemanusiaan.[17] Tujuan utamanya bukanlah untuk melarang perang, melainkan untuk mengatur cara dan metode peperangan dan untuk melindungi mereka yang tidak atau tidak lagi berpartisipasi dalam permusuhan. Fondasi HHI dibangun di atas keseimbangan antara kebutuhan militer (*military necessity*), asas kesatriaan (*chivalry*), dan pertimbangan kemanusiaan (*humanity*).[18] Dari keseimbangan ini, lahirlah prinsip-prinsip kardinal yang mengatur pelaksanaan permusuhan, di antaranya adalah prinsip pembedaan (*distinction*) dan proporsionalitas (*proportionality*). Kedua prinsip ini merupakan pilar utama yang memastikan bahwa kehancuran akibat perang tetap berada dalam batas yang dapat diterima secara hukum dan moral.

Prinsip Pembedaan (*Principle of Distinction*)

Prinsip pembedaan (*principle of distinction*) merupakan pilar fundamental dan landasan utama dalam HHI. Secara esensial, prinsip ini membebankan kewajiban kepada setiap pihak yang terlibat dalam konflik bersenjata untuk senantiasa melakukan pembedaan yang jelas antara kombatan dan penduduk sipil, serta antara objek militer dan objek sipil. Konsekuensinya, operasi militer hanya boleh diarahkan secara eksklusif terhadap sasaran militer. Landasan yuridis dari kewajiban ini terkodifikasi secara eksplisit dalam Pasal 48 Protokol Tambahan I 1977, yang menyatakan: "*In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.*"[19] Kekuatan mengikatnya dipertegas oleh statusnya sebagai hukum humaniter internasional kebiasaan yang diakui secara universal, sebagaimana

[17] Jean-Pictet, *Development and Principles of International Humanitarian Law* (Dordrecht: Martinus Nijhoff Publishers, 1985), hlm. 62.
[18] Haryomataram, *Hukum Humaniter* (Jakarta: CV Rajawali, 1984), hlm. 34.
[19] Protokol Tambahan I, *loc.cit.*

ditegaskan dalam Aturan 1 yang mengatur pembedaan antara Orang Sipil dan Kombatan dan Aturan 7 yang mengatur Pembedaan antara Objek Sipil dan Sasaran Militer.[20]

Penerapan prinsip fundamental ini ternyata menghadapi tantangan yang signifikan dalam ranah perang siber kontemporer. Sebuah "serangan" dalam konteks siber, sebagaimana didefinisikan oleh *Tallinn Manual 2.0*, adalah operasi siber yang secara wajar dapat diperkirakan menyebabkan cedera atau kematian pada orang atau kerusakan pada objek.[21] Tantangan utama berakar dari sifat infrastruktur siber yang kerap bersifat penggunaan ganda (*dual-use*). Sebagai ilustrasi, serangan terhadap sebuah pusat data (*data center*) yang secara sah menyimpan informasi logistik militer dapat secara simultan melumpuhkan layanan vital sipil, seperti sistem perbankan atau akses terhadap rekam medis rumah sakit yang bergantung pada infrastruktur fisik yang sama. Kompleksitas yuridis ini semakin mendalam mengingat Aturan 100 *Tallinn Manual 2.0* menegaskan bahwa data itu sendiri dapat dikategorikan sebagai objek.[22] Hal ini menciptakan sebuah dilema yang rumit, di mana upaya untuk membedakan antara data militer dan data sipil yang sering kali tersimpan dalam satu sistem fisik yang sama menjadi tantangan besar dalam memastikan kepatuhan terhadap prinsip pembedaan.

Prinsip Proporsionalitas (*Principle of Proportionality*)

Prinsip proporsionalitas (*principle of proportionality*) berfungsi sebagai pelengkap krusial bagi prinsip pembedaan dalam kerangka HHI. Prinsip ini mulai berlaku ketika sebuah serangan ditujukan kepada sasaran militer yang sah, namun serangan tersebut memiliki potensi untuk menimbulkan dampak sampingan (*collateral damage*) terhadap penduduk atau objek sipil. Secara fundamental, prinsip ini tidak melarang seluruh dampak sampingan, melainkan menuntut adanya keseimbangan antara keuntungan militer yang diantisipasi dengan kerugian sipil yang mungkin terjadi. Dasar hukum kewajiban ini terkodifikasi dalam Pasal 51(5)(b) Protokol Tambahan I 1977, yang secara spesifik melarang serangan "*which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage*

[20] Jean-Marie Henckaerts dan Louise Doswald-Beck, *Customary International Humanitarian Law, Volume I: Rules* (Cambridge: Cambridge University Press for the ICRC, 2005), Aturan 1 dan 7.
[21] Schmitt, *op.cit.*, 2017, Aturan 92.
[22] *Ibid.*, Aturan 100.

anticipated."[23] Kekuatan mengikatnya juga telah mengakar kuat sebagai hukum humaniter internasional kebiasaan, sebagaimana diakui dalam Aturan 14.[24]

Penerapan kalkulasi proporsionalitas ini menghadapi kompleksitas yang luar biasa dalam domain siber. Hal ini disebabkan oleh sifat efek berjenjang dan tidak langsung (*cascading and indirect effects*) yang melekat pada operasi siber, di mana dampak serangan dapat menyebar secara sistemik dan meluas dengan cara yang sulit diprediksi. Sebagai contoh, sebuah serangan siber yang berhasil melumpuhkan jaringan listrik utama di suatu wilayah perkotaan tidak hanya akan memadamkan penerangan, tetapi juga berpotensi mematikan sistem pemurnian air, menonaktifkan peralatan medis vital di rumah sakit, dan melumpuhkan jaringan komunikasi darurat.[25] *Tallinn Manual 2.0*, dalam Aturan 113, mengakui bahwa seluruh efek tidak langsung ini wajib diperhitungkan dalam analisis proporsionalitas seorang komandan, dengan syarat bahwa efek tersebut dapat diperkirakan secara wajar (*reasonably foreseeable*) pada saat serangan direncanakan.[26]

Perang Siber (*Cyber Warfare*) sebagai Domain Peperangan Modern

Perang siber merujuk pada penggunaan teknik dan teknologi siber oleh suatu negara untuk menyusup atau menyerang jaringan komputer dan sistem informasi negara lain dengan tujuan menimbulkan kerusakan yang sebanding dengan aksi militer konvensional.[27] Berbeda dengan domain peperangan tradisional (darat, laut, udara), ruang siber memiliki karakteristik unik yang menantang asumsi-asumsi dasar HHI. Pertama, ia bersifat nirbatas (*borderless*), memungkinkan serangan dilancarkan dari mana saja dan menargetkan lokasi mana pun tanpa memerlukan kehadiran fisik. Kedua, terdapat masalah atribusi (*attribution problem*) yang signifikan, di mana sulit untuk secara cepat dan definitif mengidentifikasi pelaku serangan, apakah itu aktor negara, kelompok proksi, atau entitas non-negara.

[23] Protokol Tambahan I, *op.cit.*, Pasal 51(5)(b).
[24] Henckaerts dan Doswald-Beck, *op. cit.*, Aturan 14.
[25] International Committee of the Red Cross (ICRC), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions* (2019), hlm. 26–27.
[26] Schmitt, *op.cit.*, 2017, Aturan 113, para. 5.
[27] Michael N. Schmitt, "Cyber Operations and the Jus in Bello: The Tallinn Manual," *Loyola University Chicago International Law Review* 9, no. 2 (2012): hlm. 99.

Karakteristik paling fundamental dalam konteks HHI adalah keterikatan inheren medan perang siber dengan infrastruktur sipil. Jaringan listrik, sistem perbankan, komunikasi, dan transportasi yang menjadi tulang punggung kehidupan masyarakat modern, juga merupakan infrastruktur yang digunakan oleh militer. Hal ini menciptakan lingkungan operasi di mana target militer dan objek sipil sering kali saling terkait atau bahkan berbagi infrastruktur fisik yang sama. Meskipun memiliki karakteristik yang berbeda dari peperangan kinetik, terdapat konsensus internasional yang kuat bahwa HHI tetap berlaku (*lex lata*) pada operasi siber yang terjadi dalam konteks konflik bersenjata.[28] Komite Internasional Palang Merah (ICRC) telah secara konsisten menegaskan bahwa "prinsip-prinsip HHI yang mapan berlaku untuk perang siber, meskipun klarifikasi lebih lanjut mengenai penerapannya diperlukan."[29] Oleh karena itu, perdebatan hukum tidak lagi berkisar pada *apakah* HHI berlaku, melainkan *bagaimana* prinsip-prinsip HHI yang ada diinterpretasikan dan diterapkan pada realitas teknis dan operasional serangan siber.

METODE PENELITIAN

Penelitian ini menggunakan metode hukum yuridis normatif.[30] Metode ini dipilih karena fokus penelitian adalah menganalisis norma, asas, dan prinsip hukum—khususnya prinsip pembedaan dan proporsionalitas—dan bagaimana aturan-aturan tersebut menghadapi tantangan dalam konteks teknologi perang siber. Penelitian ini menggabungkan tiga pendekatan. Pertama, pendekatan peraturan perundang-undangan (*statute approach*) yang dalam tulisan ini diaplikasikan untuk menganalisis instrumen hukum internasional yang relevan, seperti Konvensi-Konvensi Jenewa 1949 dan Protokol Tambahan I 1977. Kedua, pendekatan konseptual (*conceptual approach*) untuk mendalami makna dan ruang lingkup konsep-konsep inti seperti "pembedaan," "proporsionalitas," "serangan," dan "objek militer" dalam konteks siber. Ketiga, pendekatan kasus (*case approach*): Menggunakan konflik Rusia–Ukraina sebagai studi kasus untuk melihat bagaimana prinsip-prinsip hukum tersebut diterapkan dalam praktik serangan siber yang nyata. Bahan hukum primer dan sekunder dikumpulkan melalui studi kepustakaan (*library research*) dan penelusuran literatur digital dari sumber-sumber

[28] Schmitt, *op.cit.*, 2017, Aturan 1.
[29] ICRC, *op.cit*., hlm. 26.
[30] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana Prenada Media Grup, 2009), hlm. 35.

terpercaya. Analisis terhadap bahan-bahan hukum tersebut kemudian dilakukan menggunakan metode deskriptif-analitis.

HASIL DAN PEMBAHASAN

Kompleksitas Prinsip Pembedaan pada Infrastruktur Siber *Dual-Use*

1. Kerancuan Demarkasi Sipil-Militer dalam Infrastruktur *Dual-Use*

Prinsip pembedaan (*principle of distinction*), yang terkodifikasi dalam Pasal 48 dan 52(2) Protokol Tambahan I 1977, merupakan pilar utama HHI.[31] Prinsip ini mewajibkan pihak yang bertikai untuk secara mutlak membedakan antara kombatan dan penduduk sipil, serta antara objek militer dan objek sipil. Serangan hanya boleh ditujukan kepada objek yang berdasarkan sifat, lokasi, tujuan, atau penggunaannya memberikan kontribusi efektif terhadap aksi militer dan penghancurannya menawarkan keuntungan militer yang pasti. Secara konseptual, prinsip ini menciptakan garis demarkasi yang jelas untuk melindungi non-kombatan.

Dalam perang siber, garis demarkasi ternyata menjadi ilusi.[32] Karakteristik paling menonjol dari infrastruktur digital modern adalah sifatnya yang penggunaan ganda (*dual-use*), di mana jaringan dan sistem yang sama melayani kebutuhan militer dan sipil secara simultan. Konflik Rusia–Ukraina telah menunjukkan tantangan ini secara gamblang. Salah satu insiden paling signifikan adalah serangan siber terhadap jaringan satelit KA-SAT milik Viasat pada 24 Februari 2022, satu jam sebelum invasi darat dimulai. Serangan yang menggunakan *malware* AcidRain ini berhasil melumpuhkan puluhan ribu modem satelit.[33] Meskipun tujuannya diduga kuat untuk mengganggu komunikasi komando dan kontrol militer Ukraina, dampaknya meluas jauh ke ranah sipil. Ribuan warga sipil di Ukraina kehilangan akses internet, dan efeknya bahkan terasa di seluruh Eropa, melumpuhkan sistem pemantauan jarak jauh pada 5.800 turbin angin di Jerman.[34]

2. Dilema Larangan Serangan Indiskriminatif melalui Penggunaan *Malware Wiper*

[31] Protokol Tambahan I, *op.cit.*, Pasal 48 & Pasal 52(2).
[32] C. D. Pascucci, "Distinction and Proportionality in Cyber War," *Minnesota Journal of International Law* 26, No.2 (2017): 422–424.
[33] Andy Greenberg, "The Untold Story of the Viasat Hack, the Most Devastating Cyberattack of the Ukraine War," *Wired*, (17 November 2022).
[34] Council of the European Union, *loc.cit.*

Penggunaan *malware wiper* dirancang untuk menghancurkan data secara permanen, seperti AcidRain[35] yang menghancurkan *firmware* pada puluhan ribu modem satelit (terminal pengguna) di Ukraina dan Eropa. Dampaknya melumpuhkan layanan internet bagi pelanggan sipil dan komersial, serta secara signifikan mengganggu infrastruktur kritis, termasuk pemantauan ribuan turbin angin di Jerman. Hal ini menimbulkan masalah serius terkait prinsip pembedaan. Ketika *wiper* ini dilepaskan ke jaringan sebuah kementerian yang juga mengelola data kependudukan sipil, serangan tersebut secara inheren bersifat tanpa pandang bulu (*indiscriminate*). Menurut Komentar ICRC terhadap Protokol Tambahan I, serangan yang menggunakan metode atau sarana yang tidak dapat diarahkan pada target militer spesifik dilarang.[36] Sulit untuk membayangkan bagaimana *malware* yang menyebar secara otonom di dalam jaringan dapat dianggap sebagai senjata yang "dapat diarahkan" sesuai standar tersebut.

Insiden Viasat ini menyoroti dilema utama dalam penerapan prinsip pembedaan. Meskipun jaringan satelit tersebut dapat diklasifikasikan sebagai objek militer yang sah karena kontribusinya pada upaya perang Ukraina, serangan terhadapnya secara inheren tidak mampu membedakan antara pengguna militer dan sipil. Berbeda dengan serangan kinetik pada menara komunikasi fisik, serangan siber pada *software* atau *firmware* modem secara serentak melumpuhkan seluruh pengguna dalam jaringan tanpa diskriminasi. Hal ini menimbulkan pertanyaan fundamental: apakah sebuah serangan dapat dianggap telah mematuhi prinsip pembedaan jika metode yang digunakan secara teknis tidak memungkinkan adanya pembedaan? Doktrin HHI tradisional kesulitan menjawab pertanyaan ini, karena dirancang untuk dunia di mana objek fisik dapat diidentifikasi dan ditargetkan secara terpisah.

---

[35] Frederik A. H. Pedersen and Jeppe T. Jacobsen, "Narrow Windows of Opportunity: The Limited Utility of Cyber Operations in War," *Journal of Cybersecurity* 10, no. 1 (2024).

[36] Yves Sandoz, Christophe Swinarski, & Bruno Zimmermann (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Geneva: ICRC, 1987), para. 1978.

Implementasi Prinsip Proporsionalitas pada Serangan dengan Dampak Non-Kinetik

1. Prinsip Proporsionalitas dalam Konteks Pengukuran Dampak Non-Kinetik

Prinsip proporsionalitas, yang diatur dalam Pasal 51(5)(b) dan 57 Protokol Tambahan I 1977, melarang serangan yang dapat diperkirakan menyebabkan kerugian insidentil terhadap kehidupan sipil atau kerusakan objek sipil yang berlebihan (*excessive*) bila dibandingkan dengan keuntungan militer konkret dan langsung yang diantisipasi.[37] Prinsip ini bukan melarang *collateral damage*,[38] melainkan menuntut adanya kalkulasi penimbangan (*balancing test*) yang cermat sebelum serangan dilancarkan. Tantangan terbesar dalam menerapkan prinsip ini pada serangan siber adalah mengukur "kerusakan" non-fisik dan memprediksi efek berjenjang (*cascading effects*). Serangan siber sering kali tidak menghasilkan kawah atau puing-puing, melainkan menyebabkan disrupsi fungsional yang dampaknya merambat ke seluruh sendi kehidupan masyarakat. Sebagai contoh serangan siber NotPetya pada tahun 2017, serangan ini awalnya diluncurkan sebagai *malware* penghapus (*wiper*) yang ditargetkan secara spesifik terhadap infrastruktur kritis Ukraina, termasuk sistem perbankan, energi, dan pemerintahan, dengan disebarkan melalui kompromi *supply-chain* pada perangkat lunak akuntansi yang lazim digunakan (M.E.Doc).[39]

Desain *malware* tersebut mencakup kapabilitas *worm* (*self-propagating*) yang sangat agresif dan tidak terkendali. Akibatnya, serangan ini dengan cepat menyebar jauh melampaui yurisdiksi Ukraina dan infrastruktur militer atau pemerintah yang mungkin dianggap sebagai target sah. Jika diasumsikan terdapat "keuntungan militer yang diantisipasi" (misalnya, destabilisasi ekonomi dan pemerintahan Ukraina), kerusakan insidental yang ditimbulkannya terbukti secara nyata berlebihan. Dampak

[37] Protokol Tambahan I, *op.cit.*, Pasal 51(5)(b).
[38] Dalam HHI, *collateral damage* adalah kerugian insidentil yang timbul akibat serangan yang dilakukan selain terhadap sasaran militer yang sah ataupun kerusakan yang tidak diperkirakan sebelumnya. Prinsip ini menuntut agar dampak tersebut tidak berlebihan dibandingkan dengan keuntungan militer yang diharapkan. Lihat Gede Khrisna Kharismawan & I Made Budi Arsika, "Collateral Damage: Perlindungan Lingkungan Pada Saat Konflik Bersenjata Dalam Perspektif Deep Ecology," *Veritas et Justitia* 8, no. 2 (2022): 364.
[39] Christian Borys, "Ukraine braces for further cyber-attacks," *BBC News*, (26 Juli 2017).

rambatan (*spillover effect*)[40] dari serangan ini bersifat katastrofikal dan global. Serangan ini melumpuhkan korporasi multinasional non-militer, termasuk raksasa logistik maritim Maersk, perusahaan farmasi Merck, dan operasional FedEx (TNT Express), yang secara kolektif menderita kerugian ekonomi yang diperkirakan melampaui 10 miliar dolar AS.[41] Lebih kritis lagi, serangan ini secara langsung membahayakan kehidupan sipil di negara-negara netral dengan melumpuhkan sistem rumah sakit, seperti Heritage Valley Health System di Amerika Serikat, yang terpaksa menolak pasien dan membatalkan prosedur bedah.[42] Kerusakan ekonomi sipil global dan ancaman langsung terhadap kesehatan manusia yang masif ini jelas tidak sebanding dengan keuntungan militer regional apa pun yang mungkin dikejar, menjadikannya contoh *textbook* dari serangan siber yang melanggar prinsip proporsionalitas.

Selain NotPetya, contoh yang dapat diambil selanjutnya yaitu *malware wiper* (penghapus data) seperti WhisperGate dan gelombang serangan *Distributed Denial of Service* (DDoS) yang menargetkan sektor perbankan dan situs-situs pemerintah Ukraina pada awal 2022.[43] Meskipun serangan ini tidak menyebabkan korban jiwa secara langsung, dampaknya terhadap penduduk sipil sangat signifikan: layanan perbankan terhenti, akses terhadap informasi publik terganggu, dan timbul kepanikan massal. Secara spesifik, *malware* WhisperGate menyamar sebagai *ransomware* tetapi sejatinya bertindak sebagai *wiper* yang menimpa *Master Boot Record* (MBR), menjadikan perangkat yang terinfeksi tidak dapat dipulihkan (*irreversible*).[44] Serangan ini tidak hanya melumpuhkan sistem administrasi negara, tetapi juga menghancurkan data-data sipil yang tidak memiliki nilai militer langsung. Bersamaan dengan itu, serangan DDoS terhadap bank-bank negara terbesar, seperti PrivatBank

---

[40] N. Tavakkoli, O. Çetin, E. Ekmekcioglu & E. Savaş, "From frontlines to online: examining target preferences in the Russia–Ukraine conflict," *International Journal of Information Security*, 24, 64 (2025): 6–9.
[41] Greenberg, *loc.cit.*, 2018.
[42] *Ibid.*
[43] Microsoft Threat Intelligence Center, "Destructive 'wiper' malware," *loc.cit.*
[44] Microsoft Threat Intelligence Center, "Destructive malware targeting Ukrainian organizations," *Microsoft Security Blog*, (15 Januari 2022).

dan Oschadbank,[45] memutus akses jutaan warga sipil terhadap dana darurat mereka tepat saat ketegangan memuncak.

2. Evaluasi Penerapan Prinsip Proporsionalitas dalam Serangan Siber Konflik Rusia–Ukraina

Kasus-kasus yang telah dijabarkan sebelumnya menimbulkan pertanyaan: Bagaimana serangan ini dapat ditakar kerusakannya secara proporsional? Apakah lumpuhnya sistem perbankan selama 48 jam merupakan kerusakan yang "berlebihan" jika tujuannya adalah untuk mengganggu pendanaan logistik militer musuh? *Tallinn Manual 2.0* menegaskan bahwa efek tidak langsung yang dapat diperkirakan secara wajar (*reasonably foreseeable*) harus dimasukkan ke dalam kalkulasi proporsionalitas.[46] Namun, dalam ekosistem digital yang sangat terinterkoneksi, "kemampuan untuk memperkirakan secara wajar" menjadi sangat terbatas. Sebuah serangan pada satu sistem dapat memicu kegagalan sistemik pada sektor lain—misalnya, serangan pada sistem perbankan dapat mengganggu rantai pasokan makanan atau layanan kesehatan—dengan cara yang tidak dapat diantisipasi sepenuhnya. Dari perspektif proporsionalitas, serangan siber yang menyebabkan disrupsi luas terhadap infrastruktur kritis yang esensial bagi kelangsungan hidup penduduk sipil (*objects indispensable to the survival of the civilian population*) sangat problematis.[47] Serangan terhadap jaringan listrik, perbankan, atau bahkan jika infrastruktur tersebut juga menyuplai pangkalan militer, berisiko tinggi menyebabkan kerusakan sipil yang berlebihan. Keuntungan militer dari memadamkan listrik di sebuah markas mungkin tidak sebanding dengan penderitaan sipil yang diakibatkannya, seperti terhentinya layanan rumah sakit yang tentunya menjadi sarana vital untuk kehidupan penduduk sipil. Para ahli dalam *Tallinn Manual 2.0* sepakat bahwa efek bergema (*reverberating effects*) ini harus menjadi pertimbangan utama.[48] Konflik Rusia–Ukraina menunjukkan bahwa kalkulasi proporsionalitas dalam perang siber lebih menyerupai spekulasi daripada analisis presisi, sehingga meningkatkan risiko kerugian sipil yang tidak terduga dan tidak proporsional.

[45] Artur Korniienko, "Defense Ministry, State Banks Suffer 'Powerful' Cyberattack," *The Kyiv Independent*, (15 Februari 2022).
[46] Schmitt, *op.cit.*, 2017, Aturan 113.
[47] Hensey Fenton III, *"Proportionality and its Applicability in the Realm of Cyber Attacks," Duke Journal of Comparative & International Law* 29, no. 2 (2019).
[48] Schmitt, *op.cit.*, 2017, Aturan 113, para. 5.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan analisis yang telah diuraikan sebelumnya, dapat ditarik 2 (dua) kesimpulan mengenai tantangan penerapan prinsip pembedaan dan proporsionalitas dalam perang siber, sebagaimana terefleksikan dalam studi kasus konflik Rusia–Ukraina. Pertama, tantangan utama dalam penerapan prinsip pembedaan terletak pada sifat infrastruktur siber yang inheren berfungsi ganda (*dual-use*). Serangan terhadap target seperti jaringan satelit, sistem perbankan, atau infrastruktur energi di Ukraina menunjukkan bahwa garis demarkasi antara objek militer dan objek sipil menjadi kabur, jika bukan ilusi. Metode serangan siber sering kali secara teknis tidak mampu membedakan antara pengguna militer dan sipil dalam satu jaringan yang sama, sehingga menempatkan prinsip pembedaan pada ujian konseptual yang berat dan meningkatkan risiko serangan yang bersifat tanpa pandang bulu (*indiscriminate*).

Kedua, prinsip proporsionalitas menghadapi kendala implementasi yang tidak kalah serius. Tantangan utamanya adalah kesulitan dalam mengukur "kerusakan sipil" yang tidak bersifat fisik dan memprediksi efek berjenjang (*cascading effects*) dari sebuah serangan. Konflik Rusia–Ukraina menunjukkan bahwa dampak serangan siber melampaui kerusakan kinetik, mencakup disrupsi layanan publik esensial, kerugian ekonomi masif, dan gangguan fungsional yang meluas. Kalkulasi proporsionalitas yang diwajibkan oleh HHI menjadi sangat spekulatif ketika dampak serangan sulit dikuantifikasi dan diperkirakan *ex ante*. Dengan demikian, konflik ini secara empiris memperlihatkan bahwa kerangka hukum internasional saat ini, termasuk Protokol Tambahan I 1977 dan panduan dalam *Tallinn Manual 2.0*, meskipun bersifat fundamental, belumlah sepenuhnya memadai untuk menjawab kompleksitas peperangan modern sehingga memerlukan klarifikasi lebih lanjut untuk menjadikannya tetap relevan.

Saran

Bertolak dari kesimpulan di atas, penelitian ini merumuskan tiga saran konstruktif yang ditujukan kepada berbagai pemangku kepentingan untuk memperkuat rezim perlindungan penduduk sipil di era perang siber. Pertama, bagi komunitas internasional, khususnya Perserikatan Bangsa-Bangsa (PBB) dan Komite Internasional Palang Merah (ICRC), disarankan untuk memfasilitasi dialog multilateral antarnegara guna mencapai

pemahaman bersama (*common understanding*) mengenai interpretasi norma-norma HHI dalam konteks siber. Upaya ini dapat diwujudkan melalui pembentukan pedoman tidak mengikat (*non-binding guidelines*) atau deklarasi interpretatif yang secara konkret mengklarifikasi istilah-istilah kunci seperti "serangan", "objek militer", dan "kerusakan berlebihan" ketika diterapkan pada operasi siber. Klarifikasi ini krusial untuk mengurangi ambiguitas yang dapat dieksploitasi untuk membenarkan tindakan yang merugikan warga sipil.

Kedua, bagi para akademisi dan peneliti hukum, disarankan untuk memperdalam kajian interdisipliner yang menjembatani ilmu hukum dengan teknologi informasi, keamanan siber, dan studi strategis. Penelitian di masa depan hendaknya tidak hanya berfokus pada analisis doktrinal, tetapi juga pada pengembangan metodologi praktis untuk menilai dampak sipil dari serangan siber. Pengembangan kerangka kerja untuk analisis proporsionalitas yang lebih presisi, yang dapat digunakan oleh perencana militer, merupakan area riset yang sangat mendesak untuk dieksplorasi.

Ketiga, bagi negara-negara, baik yang terlibat konflik maupun tidak, disarankan untuk mengadopsi kebijakan nasional yang mengedepankan transparansi dan akuntabilitas dalam operasi siber militer. Hal tersebut mencakup pengembangan doktrin militer, aturan pelibatan (*rules of engagement*), dan mekanisme tinjauan (*review mechanisms*) yang secara eksplisit mengintegrasikan kewajiban berdasarkan prinsip pembedaan dan proporsionalitas. Negara-negara memiliki tanggung jawab utama untuk memastikan bahwa angkatan bersenjata mereka dilatih dan diperlengkapi untuk mematuhi HHI di semua domain peperangan, termasuk domain siber. Pada akhirnya, perkembangan teknologi tidak boleh dibiarkan mengikis fondasi kemanusiaan yang menjadi pilar hukum perang. Kolaborasi internasional dan komitmen tulus untuk menegakkan hukum adalah kunci untuk memastikan perlindungan bagi mereka yang tidak berpartisipasi dalam permusuhan di tengah medan perang abad ke-21 yang semakin kompleks.

DAFTAR REFERENSI

Buku

Dinstein, Y. (2016). *The Conduct of Hostilities under the Law of International Armed Conflict* (3rd ed.). Cambridge, United Kingdom: Cambridge University Press.

Fleck, D. (Ed.). (2013). *The Handbook of International Humanitarian Law* (3rd ed.). Oxford, United Kingdom: Oxford University Press.

Haryomataram. (1984). *Hukum Humaniter*. Jakarta: CV Rajawali.

Henckaerts, J.-M., & Doswald-Beck, L. (2005). *Customary International Humanitarian Law, Volume I: Rules*. Cambridge, United Kingdom: Cambridge University Press for the ICRC.

Marzuki, P. M. (2009). *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group.

Pictet, J. (1985). *Development and principles of international humanitarian law*. Dordrecht, Netherlands: Martinus Nijhoff Publishers.

Instrumen Hukum Internasional

Charter of the United Nations. (1945). 1 U.N.T.S. XVI.

Convention (IV) relative to the Protection of Civilian Persons in Time of War. (1949). 75 U.N.T.S. 287.

Protokol Tambahan pada Konvensi Jenewa 12 Agustus 1949, dan yang berhubungan dengan Perlindungan Korban-korban Pertikaian Bersenjata Internasional (Protokol I). (1977). 1125 U.N.T.S. 3.

Jurnal Ilmiah

Chen, S., Hao, M., Ding, F., & et al. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications, 10*, 71.

Fenton, H. III. (2019). Proportionality and its applicability in the realm of cyber attacks. *Duke Journal of Comparative & International Law*, 29(2), 335-359.

Finlay, L., & Payne, C. (2019). The attribution problem and cyber armed attacks. *American Journal of International Law, 113*, 202-206.

Hakala, J. (2023). Cyber operations in the Russo-Ukrainian War: A challenge to the existing legal order? *Journal of Conflict & Security Law, 28*(1), 121–143.

Hathaway, O. A., Khan, A., & Revkin, M. R. (2025). The dangerous rise of “dual-use” objects in war. *Yale Law Journal*, *134*(8).

Jensen, E. T. (2021). The principle of distinction and cyber operations: Gray areas and difficult questions. *International Law Studies, 97*, 998-1025.

Kharismawan, G. K., & Arsika, I. M. B. (2022). Collateral damage: Perlindungan lingkungan pada saat konflik bersenjata dalam perspektif deep ecology. *Veritas et Justitia, 8*(2), 362–385.

Lin, H. (2013). Cyber conflict and international humanitarian law. *International Review of the Red Cross, 94*(886), 515–531.

Lin, H. (2022). Russian cyber operations in the invasion of Ukraine. *The Cyber Defense Review, 7*(4), 31–46.

Pascucci, C. D. (2017). Distinction and proportionality in cyber war. *Minnesota Journal of International Law, 26*(2).

Pedersen, F. A. H., & Jacobsen, J. T. (2024). Narrow windows of opportunity: The limited utility of cyber operations in war. *Journal of Cybersecurity, 10*(1), tyae014.

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). *Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure*. *Sensors, 23*(9), 4060.

Schmitt, M. N. (2012). Cyber operations and the jus in bello: The Tallinn Manual. *Loyola University Chicago International Law Review, 9*(2), 99-122.

Shereshevsky, Y. (2022). *International humanitarian law-making and new military technologies*. *International Review of the Red Cross, 104*(920–921), 273–302.

Tavakkoli, N., Çetin, O., Ekmekcioglu, E., & Savaş, E. (2025). From frontlines to online: Examining target preferences in the Russia–Ukraine conflict. *International Journal of Information Security, 24*(64), 1–15.

Tsagourias, N. (2018). The principle of proportionality in cyber operations. *International Law Studies, 94*, 39-65.

Komentar dan Manual

Sandoz, Y., Swinarski, C., & Zimmermann, B. (Eds.). (1987). *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Geneva, Switzerland: Martinus Nijhoff Publishers for the ICRC.

Schmitt, M. N. (Gen. Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, United Kingdom: Cambridge University Press.

Laporan dan Dokumen Resmi

Chivvis, C. S. (2017). *Understanding Russian "Hybrid Warfare"*. Santa Monica, CA: RAND Corporation. Diakses dari https://www.rand.org/pubs/testimonies/CT468.html

Council of the European Union. (10 Mei 2022). *Declaration by the High Representative on behalf of the European Union on malicious cyber activity conducted by the Russian Federation against Ukraine*. Diakses dari https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russia-s-malicious-cyber-activity-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-eu/

International Committee of the Red Cross. (2019). *International humanitarian law and the challenges of contemporary armed conflicts: Recommitting to protection in armed conflict on the 70th anniversary of the Geneva Conventions*. Diakses dari https://www.icrc.org/sites/default/files/document/file_list/challenges-report_new-technologies-of-warfare.pdf

North Atlantic Treaty Organization (NATO). (30 Juli 2024). *Cyber defence*. Diakses dari https://www.nato.int/cps/en/natohq/topics_78170.htm

U.S. Department of Justice. (19 Oktober 2020). *Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace*. Diakses dari https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

Sumber dari Internet dengan Nama Penulis

Borys, C. (26 Juli 2017). *Ukraine braces for further cyber-attacks*. BBC News. Diakses dari https://www.bbc.com/news/technology-40706093

Greenberg, A. (17 November 2022). *The untold story of the Viasat hack, the most devastating cyberattack of the Ukraine war*. Wired. Diakses dari https://www.wired.com/story/viasat-hack-ukraine-russia-most-devastating-cyberat tack/

Greenberg, A. (22 Agustus 2018). *The untold story of NotPetya, the most devastating cyberattack in history*. Wired. Diakses dari https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Korniienko, A. (15 Februari 2022). *Defense Ministry, state banks suffer 'powerful' cyberattack.* The Kyiv Independent. Diakses dari https://kyivindependent.com/defense-ministry-state-banks-suffer-powerful-cyberattack/

Sumber dari Internet tanpa Nama Penulis

Microsoft Threat Intelligence Center. (15 Januari 2022). *Destructive malware targeting Ukrainian organizations*. Microsoft Security Blog. Diakses dari https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

Microsoft Threat Intelligence Center. (24 Februari 2022). *Destructive 'wiper' malware targeting Ukrainian organizations*. Microsoft Blog. Diakses dari https://www.microsoft.com/en-us/security/blog/2022/02/24/destructive-malware-targeting-ukrainian-organizations/