DIPONEGORO LAW JOURNAL
Volume 13, Nomor 3, Tahun 2024
Website : https://ejournal3.undip.ac.id/index.php/dlr/

PERTANGGUNGJAWABAN RUSIA ATAS TINDAKANNYA MELAKUKAN CYBER WARFARE DALAM KONFLIK BERSENJATA DENGAN UKRAINA BERDASARKAN HUKUM HUMANITER INTERNASIONAL

RM. Andrew Cahyo Junior, Nuswantoro Dwiwarno, Pulung Widhi Hari Hananto
Program Studi S1 Hukum, Fakultas Hukum, Universitas Diponegoro
E-mail : andrewcjunior@gmail.com

Abstrak

Cyber warfare terhadap Ukraina mengakibatkan melemahnya kemampuan pemerintah dan militer untuk berkomunikasi serta beroperasi, akibatnya legitimasi dan otoritas institusi politik dan militer Ukraina ikut terdampak. Tujuan penelitian ini untuk mengetahui pengaturan tentang *cyber warfare* dalam konflik bersenjata menurut hukum humaniter internasional dan analisis pertanggungjawaban hukum terhadap Rusia yang telah melakukan *cyber warfare*. Metode penelitian yang digunakan adalah yuridis normative. Spesifikasi penelitian dalam penelitian ini adalah deskriptif analitis. Penelitian ini menggunakan jenis data sekunder. Hasil penelitian yang telah dilakukan didapati hasil bahwa pengaturan tentang *Cyberwarfare* dalam konflik bersenjata menurut Hukum Humaniter Internasional didasarkan pada Pasal 22 dan Pasal 23 Konvensi Den Haag 1907, Pasal 35 dan 36 Protokol I/1977, dan Konvensi Senjata termasuk *Tallinn Manual on the International Law Applicable to Cyber Warfare* ("*Tallinn Manual* 1.0"). Pertanggungjwaban hukum terhadap Rusia didasarkan pada Konvensi Jenewa 1949 di mana Rusia sebagai anggota PBB telah meratifikasi konvensi ini.

Kata Kunci: *Cyberwarfare*; Hukum Humaniter Internasional; Kejahatan Perang.

Abstract

Cyber warfare against Ukraine resulted in a weakening of the government and military's ability to communicate and operate, as a result the legitimacy and authority of Ukraine's political and military institutions were affected. The aim of this research is to determine the regulation of cyber warfare in armed conflict according to international humanitarian law and to analyze legal responsibility for Russia which has carried out cyber warfare. The research method used is normative juridical. The research specifications in this study are analytical descriptive. This research uses secondary data. The results of the research that has been carried out show that the regulation of Cyberwarfare in armed conflict according to International Humanitarian Law is based on Article 22 and Article 23 of the 1907 Hague Convention, Articles 35 and 36 of Protocol I/1977, and the Weapons Convention including the Tallinn Manual on the International Law Applicable to Cyber Warfare ("Tallinn Manual 1.0"). Legal responsibility for Russia is based on the 1949 Geneva Convention where Russia as a member of the UN has ratified this convention.

Keywords: *Cyberwarfare; International Humanitarian Law; War Crimes.*

DIPONEGORO LAW JOURNAL
Volume 13, Nomor 3, Tahun 2024
Website : https://ejournal3.undip.ac.id/index.php/dlr/

I. PENDAHULUAN

A. Latar Belakang

Cyber warfare dapat melibatkan organisasi-organisasi, perusahaan, dan militer dalam melakukan perusakan atau menyerang sistem komputer negara lain atau pihak lain[1] Seperti halnya Rusia mengintegrasikan *cyber warfare* sebagai suatu strategi militer dan keamanan yang lebih luas guna menjadikan dunia maya sebagai 'medan perang'. Sebagaimana penyusunan strategi yang dicanangkan oleh Rusia, dimana operasi informasi IO dan militer asimetris taktik Rusia digunakan untuk mengacaukan pemerintahan negara lain, mengatur anti-pemerintahan di negaranya sendiri, menipu lawan, memengaruhi opini publik, dan mengurangi suatu *interest* dari negara lain untuk melawannya.[2]

Pada April dan Mei 2007 diketahui terjadi serangan DDos dari Rusia terhadap Estonia yang mengakibatkan selama 1 (satu) bulan situs internet Estonia terkendala *ping* serta terjadi penyumbatan jaringan data yang mana mengakibatkan pemerintah Estonia harus memutuskan koneksi internet internasional mereka. Dampak yang ditimbulkan dari *cyber warfare* oleh Rusia tersebut mengakibatkan sekitar 60% dari 1,3juta penduduk mengalami dampaknya secara virtual, psikologis, dan nyata.[3]

Adanya *cyber warfare* yang dilakukan oleh Rusia disebabkan karena serangan balasan atas tindakan pemerintah Estonia yang memindahkan patung perunggu Tentara Soviet dari Ibu Kota Tallin ke pemakaman militer yang diindikasikan oleh Rusia sebagai kecaman terhadap Tentara Soviet dalam pembebasan Estonia dari Nazi Jerman sebagai penghinaan terhadap etnis minoritas Estonia Rusia. Akibatnya, pada 27 April 2007 juga terjadi protes dan demonstrasi besar-besaran oleh etnis Rusia di Estonia yang mengakibatkan penangkapan terhadap 1.300 orang dan kematian 1 orang.

Kemudian pada tahun 2008 Rusia juga melakukan *cyber warfare* terhadap Georgia yang dimulai ketika Rusia melakukan invasi darat, udara, dan laut dalam skala besar pada 8 Agustus 2008. Kejadian ini merupakan serangan yang mirip dengan serangan Estonia pada 2007, serangan Stuxnet melumpuhkan pembangkit nuklir Bushehr dengan worm tahun 2010.[4]

Cyber warfare oleh Rusia mengakibatkan komunikasi pemerintah dan situs web pemerintah menjadi terputus, kebocoran database Bank Georgia serta perusahaan transportasi dan telekomunikasi. Rusia pada serangannya kali ini berafiliasi dengan Turki dan RBN serta Kremlin dalam hal fasilitator serangan terhadap Estonia.[5] Akibat serangan dari Rusia tersebut, Georgia mengalami suatu

---

[1] Miko Aditiya Suharto, "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional," *Jurnal Risalah Hukum* Vol17, no. 2 (2021), halaman 104.
[2] Margarita Levin Jaitner, *Cyber War in Perspective: Russian Aggression Against Ukraine* (Tallin: CEO Publications, 2015), halaman 89.
[3] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," 2022, http://www.wired.com/2007/08/ff-estonia/, diakses tanggal 06 Juni 2024.
[4] Erwin Kurnia, *Kebijakan Straegi Keamanan Cyber Nasional Dalam Menghadapi Perang Cyber (Cyber Warfare)* (Jakarta: Universitas Pertahanan Indonesia, 2014), halaman 3.
[5] John Markoff, "Before the Gunfire, Cyberattacks," 2022, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0, diakses tanggal 06 Juni 2024.

infrastruktur terbatas pada 2008 serta dampak pengalihan lalu lintas menuju server negara lain. Atas dasar tersebut, dapat disimpulkan bahwa serangan Rusia terhadap Georgia merupakan operasi *cyber* yang dilakukan bersamaan dengan serangan militer yang konvensional.

Serangan Rusia yang tidak hentinya mengakibatkan perhatian dunia Internasional yakni terhadap Ukraina sejak tahun 2013 hingga sekarang. *Cyber warfare* terhadap Ukraina mengakibatkan melemahnya kemampuan pemerintah dan militer untuk berkomunikasi serta beroperasi, akibatnya legitimasi dan otoritas institusi politik dan militer Ukraina ikut terdampak. Peretas Rusia menggunakan *spear phishing, malware, DDoS Attack, TdoS,* dan spionase untuk menargetkan pemerintahan Ukraina guna membocorkan dokumen dan rencana pemerintah yang juga berdampak terhadap publik.[6] Selain itu pada tahun 2015, Rusia menggunakan akses jarak jauh untuk mengontrol dan mengoperasikan sistem yang menyebabkan pemadaman listrik sehingga berdampak pada aktifitas 220.000 penduduk Ukraina.

Seiring dengan berkembanganya teknologi mengakibatkan metode serta persenjataan yang digunakan dalam konflik bersenjata juga mengalami perkembangan.[7] Pengaturan berkaitan dengan *cyber warfare* belum diatur dalam Hukum Humaniter Internasional, dimana penggunaan *cyber warfare* tidak dapat dibenarkan jika melanggar metode perang sebagaimana diatur dalam Hukum Humaniter Internasional, seperti menyerang objek sipil dalam konflik bersenjata.[8]

Terdapat pengaturan dalam Pasal 25 dan Pasal 27 Konvensi Den Haag IV Tahun 1907, dimana terdapat kewajiban suatu negara dalam penggunan senjata perang guna memastikan penggunaannya tidak menimbulkan penderitaan terhadap penduduk sipil.[9] Atas dasar tersebut dalam serangan siber yang dilakukan oleh Rusia hendaknya mempertimbangkan efek dari penggunaannya agar tidak menimbulkan penderitaan terhadap penduduk sipil.

Berdasarkan serangan Rusia terhadap beberapa negara di atas, diketahui bahwa *cyber warfare* Rusia berdampak terhadap orang sipil maupun obyek sipil. Penelitian ini akan membahas mengenai pengaturan hukum humaniter internasional yang mana belum mengatur secara spesifik mengenai *cyber warfare* untuk menganalisis kekosongan yang terjadi guna menentukan aktor dalam *cyber warfare,* sejauh mana batasan dari *cyber warfare* dapat dilakukan, metode *cyber warfare* yang diperbolehkan oleh hukum humaniter internasional guna membatasi warga sipil terkena dampaknya. Untuk itu penelitian ini berfokus pada pembahasan dengan judul **"Pertanggungjawaban Rusia Berdasarkan Hukum**

---

[6] Azhar Unwala dan Shaheen Gori, "Brandishing the Cybered Bear: Information War and Russian-Ukraine Conflict," *Military Cyber Affairs* vol. 1, no. 1 (2015), halaman 7.
[7] Vincent Bernard, "Tactics, Techniques, Tragedies: A Humanitarian Perspective on Thr Changing Face to War," *International Review of The Red Cross* vol. 97, no. 900 (2015), halaman 959–968.
[8] Joko Setiyono dan Nuswantoro Dwiwarno Raka Permana Nayaspoetra, "Perlindungan Objek Sipil Atas Penggunaan Cyber Warfare Dalam Konflik Bersenjata Antara Rusia Dengan Ukraina Dalam Perspektif Hukum Humaniter Internasional," *Diponegoro Law Journal*, 2019, halaman 1.
[9] dan Kabul Supriyadhie Yohana Tri Meiliyani, Joko Setiyono, "Kajian Hukum Humaniter Internasional Mengenai Cyber Warfare Dalam Konflik Bersenjata Internasional Antara Israel Dan Palestina Atas Gaza," *Diponegoro Law Journal* vol. 8, no. 2 (2018), halaman 1598.

Humaniter Internasional atas Tindakannya Telah Melakukan *Cyber Warfare* dalam Konflik Bersenjata dengan Ukraina".

B. Kerangka Teori

1. Teori Hukum Humaniter Internasional

Istilah Hukum Humaniter Internasional (*International Humanitarian Law*) dalam kajian Hukum Internasional senantiasa mengalami perubahan dari waktu ke waktu. Diawali dengan istilah Hukum Perang (*Laws of War*), yang kemudian berubah menjadi Hukum Konflik Bersenjata (*Laws of Armed Conflicts*) merupakan salah satu cabang dari hukum internasional publik, yaitu cabang hukum yang mengatur masalah-masalah lintas batas antar negara.[10]

Jean Pictet, mendefinisikan Hukum Humaniter Internasional sebagai "*International Humanitarian Law in the wide sense is constitutional legal provision, whether written and customary. Ensuring respect for individual and his well-being*." Hukum Humaniter Internasional tersebut menurut Jean Pictet intinya merupakan tentang penghormatan terhadap setiap individu. [11]

Mochtar Kusumaatmadja juga mengemukakan pembagian hukum perang menjadi 2 (dua) bagian, yakni:[12]

a. *Ius ad bellum* yaitu hukum tentang perang, mengatur tentang bagaimana Negara dibenarkan menggunakan kekerasan bersenjata; dan
b. *Ius ad bello* yaitu hukum yang berlaku dalam perang. *Ius ad bello* dibagi lagi menjadi:
    1) Hukum yang mengatur cara dilakukannya perang *(the conduct of war),* bagian ini disebut *The Hague Laws.*
    2) Hukum yang mengatur perlindungan orang-orang yang menjadi korban perang, bagian ini disebut *The Geneva Laws.*

Selain pendapat dari para ahli di atas, ada juga para ahli yang mempunyai pendapat mengenai hukum humaniter, antara lain Esbjorn Rosenbland yang pada intinya merumuskan bahwa Hukum Humaniter Internasional tidak hanya sekedar tentang tata cara dan metoda dalam berperang saja, tetapi juga mengatur tentang perlindungan korban-korban perangnya.[13]

HukumHumaniterInternasional mengenal beberapa prinsip penting yang berasal dari Hukum Kebiasaan Perang, dimana prinsip-prinsip ini kemudian menjadi dasar dalam penyusunan peraturan maupun perjanjian internasional yang terkait Hukum Humaniter Internasional. Prinsip dalam Hukum Kebiasaan Perang antara lain.[14] Adapun penjelasan prinsip-prinsip Hukum Humaniter Internasional tersebut berupa:

---

[10] Wahyu Wagiman, *Hukum Humaniter Dan HAM* (Jakarta: : Lembaga Studi dan Advokasi Masyarakat, 2005), halaman 4.
[11] Herman Suryokumoro, *Hukum Humaniter Internasional: Kajian Norma Dan Kasus* (Malang: Brawijaya University Press, 2020), halaman 5.
[12] Haryomataram, *Pengantar Hukum Humaniter* (Jakarta: Rajawali Press, 1994), halaman 6.
[13] Esbjorn Rosenbland dalam Rafika Mayasari Siregar, "Tinjauan Yuridis Konvensi Jenewa IV Tahun 1949 Terhadap Negara-Negara Yang Berperang Menurut Hukum Internasional," *Sumatra Journal of International Law*, 2013, halaman 7.
[14] Haryomataram, *Hukum Humaniter* (Jakarat: Rajawali Press, 1984), halaman 4.

a. Prinsip Kepentingan Militer (*Military Neccessity Principle*)
   Prinsip Kepentingan Militer ini diatur dalam *Customary International Humanitarian Law* (*Customary IHL*) *Rule* 14.[15]
b. Prinsip Pembatasan (*Limitation Principle)*
   Prinsip Pembatasan adalah suatu prinsip yang menghendaki adanya pembatasan terhadap sarana atau alat serta cara atau metode berperang yang dilakukan oleh pihak yang bersengkata, seperti adanya larangan penggunaan racun atau senjata beracun, larangan penggunaan peluru dum-dum, atau larangan menggunakan suatu proyektil yang dapat menyebabkan luka-luka yang berlebihan (*superfluous injury)* dan penderitaan yang tidak perlu (*unnecessary suffering),* dan lain-lain.[16]
c. Prinsip Proporsional (*Proportionality Principle)*
   Prinsip Proporsional adalah prinsip yang diterapkan untuk membatasi kerusakan yang disebabkan oleh operasi militer dengan mensyaratkan bahwa akibat dari sarana dan metode berperang yang digunakan tidak boleh tidak proporsional (harus proporsional) dengan keuntungan militer yang diharapkan.[17]
d. Prinsip Kesatriaan (*Chivalry Principle*)
   Prinsip ini mengandung arti bahwa di dalam suatu peperangan, kejujuran harus diutamakan. Penggunaan alat-alat yang ilegal atau bertentangan dengan Hukum Humaniter serta cara-cara berperang yang bersifat khianat dilarang.[18]
e. Prinsip Pembedaan (*Distinction Principle*)

Pada dasarnya, pada setiap kondisi konflik bersenjata, hanya terdapat dua macam status seseorang, yaitu apakah ia berstatus sebagai penduduk sipil (non-kombatan) atau sebagai kombatan *(combatant).* Prinsip Pembedaan ini bersangkutan dengan status seseorang dalam suatu keadaan konflik bersenjata sebagaimana diatur dalam Pasal 2 Protokol Tambahan I Konvensi Jenewa 1977 bahwa penduduk sipil dan kombatan tetap berada di bawah perlindungan dan wewenang dari prinsip Hukum Internasional. Berdasarkan prinsip ini pada waktu terjadi perang atau konflik bersenjata harus dilakukan pembedaan antara penduduk sipil dengan kombatan serta antara objek sipil dengan objek militer, warga sipil adalah orang yang tidak memakai atribut militer dan tidak ikut serta dan tidak punya andil dalam konflik bersenjata, dan yang dimaksud obyek sipil adalah semua obyek yang tidak memiliki sumbangan yange fektif bagi aksi-aksi militer, yang jika dihancurkan secara total atau sebagian, direbut atau dinetralisasi, tidak memberikan keuntungan militer yang pasti. Berdasarkan prinsip ini hanya kombatan dan objek militer yang boleh dijadikan sasaran. Banyak ahli yang

[15] ICRC, "Rule 14 Proportionality in Attack," 2022, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule14, diakses tanggal 06 Juni 2024.
[16] dan Saartje Mandagi Wagiman, Anasthasya, *Terminologi Hukum Internasional* (Jakarta: Sinar Grafika, 2016), halaman 45.
[17] I. Gst Ngr Hady Purnama Putera, "Penggunaan Exoskeleton Sebagai Senjata Dalam Konflik Bersenjata Internasional Di Masa Yang Akan Datang Ditinja Dari Prinsip-Prinsip Hukum Humaniter Internasional," *Jurnal Komunikasi Hukum* vol.2, no. 2 (2016), halaman 185.
[18] Haryomataram, *Op.Cit.,* halaman 34.

berpendapat bahwa prinsip pembedaan ini adalah yang paling penting dalam prinsip-prinsip hukum humaniter.[19]

2. Teori Tentang *Cyberwarfare*

Dalam uraian pada sub bab sebelumnya diketahui bahwa *Cyber Warfare* merupakan bagian dari serangan *cyber* yang terjadi di dunia maya. Sebagai informasi bahwa berkaitan mengenai tindakan *cyber crime* atau serangan siber yang kerap terjadi di beberapa negara, sehingga membuat negara-negara di dunia menjadi khawatir akan terjadinya hal tersebut maka hal ini mendorong *Council of Europe* untuk memprakarsai pembentukan konvensi tentang kejahatan *cyber*.[20]

Cyber warfare terjadi dalam sebuah ruang yang disebut *cyber space* atau ruang siber. Adapun pengertian *cyber space* itu sendiri muncul sejak tahun 1984 sebagaimana dikemukakan oleh William Gibson.[21] Kemudian Kementerian Pertahanan Amerika Serikat memberikan definisi mengenai *cyber space* yang diartikan sebagai sebuah ruang dimana informasi digital saling berkomunikasi melalui jaringan komputer dan baik pihak sipil, militer, maupun teroris sekalipun melakukan berbagai urusannya.[22]

Richard Clarke yang memberikan definisi mengenai *cyber warfare* berupa: *"... actions by a nation-state to penetrate another nation's computer or networks for the purposes of causing damage or disruption*".[23] Atau dapat diartikan, suatu tindakan oleh negara untuk menembus jaringan negara lain dengan tujuan menimbulkan kerusakan atau gangguan.

Selanjutnya, ICRC turut memberikan pengertian mengenai *cyber warfare* yang diartikannya sebagai suatu bentuk operasi terhadap musuh melalui komputer dengan maksud menghancurkan, merusak, atau menganggu.[24] Berangkat dari pendapat Richard Clarke dan ICRC tersebut dapat dikatakan bahwa *cyber warfare* memiliki tujuan untuk mencapai suatu kerugian terhadap negara atau pihak lain baik itu dari segi militer maupun bisnis.

Cyber warfare termasuk ke dalam operasi siber atau *cyper operation* yang diartikan sebagai suatu bentuk operasi yang bertujuan untuk memproyeksikan kekautan di dan melalui *cyber sapce* guna memanipulasi, menganggu atau menghancurkan target.[25] Sehingga dapat disimpulkan bahwa operasi siber memiliki tujuan guna menganggu, memanipulasi atau menghancurkan target

---

[19] Jean Pictet, "The Fundamental Principles of the Red Cross: Commentary," *International Review of The Red Cross* vol. 19, no. 210 (1979), halaman 6.
[20] Sayid Qutub, *Cyber Terrorism Dalam Hukum Islam* (Jakarta: Irama Offset, 2015), halaman 25.
[21] Andrew D. Murray, *The Regulation of Cyberspace: Control in The Online Environment* (Abingdon: Routledge-Cavendish, 2007), halaman 5.
[22] Steve Winterfeld, *The Basic of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (Amsterdam: Syngress, 2013), halaman 6.
[23] Richard Clarke dan Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins Publishers, 2010), halaman 823.
[24] ICRC, "The Evolution of Warfare," *International Review of The Red Cross* vol. 97, no. 900 (2015), halaman 1473.
[25] Bart Hagoyen dan Fergus Hanson Tom Urent, "Defining Offensive Cyber Capabilities," 2022, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities, halaman 06 Juni 2024.

untuk mencapai suatu tujuan yang besar serta memiliki dampak terhadap dunia nyata.

C. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan pada pembahasan sebelumnya, untuk itu penulis merumuskan permasalahan penelitian berupa:

1. Bagaimanakah pengaturan tentang *cyber warfare* dalam konflik bersenjata menurut hukum humaniter internasional?
2. Bagaimanakah pertanggungjawaban hukum terhadap Rusia yang telah melakukan *cyber warfare* dalam konflik bersenjata dengan Ukraina?

II. METODE PENELITIAN

Penelitian adalah suatu kegiatan ilmiah yang ada kaitannya dengan analisa dan konstruksi yang dilakukan secara metodologis, sistematis dan konsisten. Metodologi berarti sesuai dengan metode atau cara tertentu, sistematis berarti berdasarkan suatu sistem, sedangkan konsisten berarti tidak adanya hal-hal yang bertentangan dengan suatu kerangka.[26] Penulisan hukum ini menggunakan metode penelitian sebagai berikut:

A. Jenis Penelitian

Jenis penelitian ini adalah doktrinal, yaitu berdasarkan kaidah-kaidah hukum. Disebut penelitian hukum doktrinal, karena penelitian ini dilakukan atau ditujukan hanya pada peraturan-peraturan yang tertulis atau bahan-bahan hukum. Sedangkan disebut sebagai penelitian kepustakaan ataupun studi dokumen, disebabkan penelitian ini lebih banyak diakukan terhadap data yang bersifat sekunder.[27]

B. Metode Pendekatan

Tipe pendekatan yang digunakan dalam yuridis normatif yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan *(statute approach)*. Pendekatan ini dilakukan dengan menelaah semua peraturan perundang-undangan dan regulasi yang terkait dengan isu hukum yang sedang dibahas (diteliti).[28]

C. Spesifikasi Penelitian

Spesifikasi penelitian yang digunakan dalam penelitian ini adalah deskriptif analitis. Deskriptif analitis menurut Sugiyono, yaitu metode yang digunakan untuk memberikan gambaran atau melakukan analisa terhadap suatu penelitian namun hal tersebut tidak digunakan untuk membuat suatu kesimpulan secara lebih luas.[29]

---

[26] Muhammad Syahrum, *Pengantar Metodologi Penelitian Hukum* (Riau: Dotplus Publisher, 2022), halaman 10.
[27] W Gulo, *Metodologi Penelitian* (Jakarta: Grasindo, 2019), halaman 42.
[28] Nurul Qamar, *Metode Penelitian Hukum* (Makassar: Social Politics Genius, 2017). halaman 19.
[29] Bambang Sunggono, *Metodologi Penelitian Hukum* (Jakarta: Raja Grafindo, 2017), halaman 26.

D. Jenis dan Sumber Data

Sesuai dengan jenis penelitian ini berupa yuridis normatif, maka dalam penelitian ini menggunakan jenis data sekunder berupa bahan-bahan hukum.[30] Menurut Amirudin dan Zainal Asikin, sumber penelitian hukum normatif hanyalah data sekunder, yang terdiri dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier.[31]

E. Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini berupa penelitian kepustakaan. Penelitian kepustakaan *(Library Research)* menurut Peter Mahmud adalah kajian terhadap berbagai informasi yang bersifat tertulis dan berkaitan dengan hukum dimana info ini didapat dari bermacam sumber dan kemudian dipublikasi meluas.[32]

F. Teknik Analisis Data

Analisis deskriptif kualitatif digunakan karena data yang dicari dan diolah merupakan data yang bersifat deskriptif dimana penulis akan mengungkapkan pembahasan mengenai fokus penelitian dalam upaya penjawaban rumusan masalah.

III. HASIL DAN PEMBAHASAN

A. Pengaturan Tentang *Cyberwarfare* dalam Konflik Bersenjata menurut Hukum Humaniter Internasional

1. Pengaturan Penggunaan Senjata Dalam Perang Menurut Hukum Humaniter

Konflik bersenjata telah banyak terjadi di dunia pada beberapa waktu yang lalu baik yang telah berlangsung lama maupun yang baru saja terjadi. Dahulu ketika negara-negara melakukan peperangan senjata dasar yang digunakan hanya sebatas bahan peledak maupun senjata api dan senjata rakitan lainnya namun seiring perkembangan waktu ditambah hadirnya Revolusi Industri, penggunaan senjata dalam berperang tidak hanya sebatas senjata-senjata tersebut, terdapat pembaharuan senjata yang digunakan saat berperang, dimana senjata ini memiliki sifat lebih merusak daripada yang dahulu.

Senjata yang digunakan seiring perkembangan zaman berkembang menjadi senjata kimia, bahan peledak dengan tingkat *explotion* yang besar dan memiliki daya rusak tinggi, senjata virus, dan termasuk senjata dalam dunia maya.

Senjata baru tersebut memiliki ciri khas yang sama yakni memiliki daya rusak yang tinggi dan berpotensi mengakibatkan timbulnya korban jiwa yang sangat banyak.

---

[30] Beni Ahmad Saebani, *Metode Penelitian Kualitatif* (Bandung: Pustaka Setia, 2019), halaman 35.
[31] Trisna Rukhmana, *Metode Penelitian Kualitatif* (Batam: Rey Media Grafika, 2022), halaman 28.
[32] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana Prenada Media Group, 2013), halaman 54.

Berkaitan dengan permasalahan pembatasan pengaturan penggunaan senjata perang tersebut, terdapat beberapa sumber hukum yang menjadi dasar pembatasan penggunaan senjata dalam konflik bersenjata antar negara menurut hukum humaniter, berikut uraiannya:[33]

a. Konvensi Den Haag Konvensi Den Haag 1899 *(The Hague Conventions)* membahas mengenai tata cara berperang.
   Konvensi ini lahir dari hasil konferensi Perdamaian I yang dilaksanakan pada 20 Mei hingga 29 Juli 1899 di Den Haag, Belanda. Konferensi yang dimulai pada tanggal 20 Mei 1899 itu berlangsung selama 2 bulan menghasilkan tiga konferensi dan tiga deklarasi pada tanggal 29 Juli 1899. Pada konvensi ini belum memiliki bentuk yang sempurna tentang pembatasan penggunaan senjata dalam berperang. Oleh sebab itu kemudian dilakukan konvensi Den Haag selanjutnya yakni Konvensi Den Haag 1907.
b. Konvensi Den Haag II Tahun 1907 atau Konvensi IV
   Aturan lainnya yang mengatur mengenai pembatasan penggunaan senjata ada pada Konvensi Den Haag II 1907 atau Konvensi IV tentang kebiasaan dalam perang darat. Konvensi ini merupakan lanjutan dari Konvensi Den Haag tahun 1899. Dalam konvensi ini terdapat pembatasan penggunaan senjata yang diatur di Pasal 22 Konvensi Den Haag 1907 yang berbunyi, *"The right of belligerents to adopt means of injuring the enemy is not unlimited".* Ini berarti bahwa ada cara-cara tertentu dan alat-alat tertentu yang dilarang untuk dipakai/digunakan.[34]
   Pengaturan lainnya ada di Pasal 23 dimana negara yang hendak menyerang negara lawan tidak diperbolehkan menggunakan alat yang dapat melukai musuh secara berkepanjangan. Contoh alat yang dilarang untuk digunakan dalam berperang menurut konvensi ini seperti larangan penggunaan racun, senjata beracun, larangan menggunakan senjata seperti proyektil atau material lainnya yang berpotensi memberikan rasa sakit yang berkepanjangan.[35]
   Dalam pasal tersebut juga mengatur tentang metode perang, di mana metode perang yang dilarang untuk digunakan adalah melukai pihak musuh dengan cara curang dan berkhianat atau membunuh, menyerang musuh yang telah menyerah. Metode perang yang demikian tidak boleh dilakukan ketika terjadi konflik peperangan antar negara.
c. Konvensi Jenewa Tahun 1977 (Protokol Tambahan I)
   Konvensi dalam hukum humaniter lainnya yang mengatur tentang pembatasan penggunaan senjata dalam peperangan adalah Konvensi Jenewa Tahun 1977 yang tertuang dalam Protokol Tambahan I. Protokol tambahan I ini dibentuk diawali adanya perkembangan metode dalam peperangan. Dalam protokol ini ditentukan bahwa para pihak yang saling bersengketa dalam konflik bersenjata memiliki batasan dalam menentukan alat atau senjata dalam perang, dimana tidak boleh menggunakan proyektil yang akan berdampak luka-luka secara

[33] *Ibid.*
[34] Pasal 22 Konvensi Den Haag 1907.
[35] Pasal 23 Konvensi Den Haag 1907.

berlebihan dan memberikan penderitaan yang teramat sangat bagi korban yang terkena proyektil.[36]

Pengaturan mengenai pembatasan senjata yang digunakan ada pada Pasal 35 Protokol Tambahan I/1977. [37] Dalam pasal tersebut dijelaskan bahwa pada dasarnya masing-masing negara yang terlibat konflik bersenjata memiliki hak untuk memilih alat untuk berperang, namun tetap terbatas bahwa dilarang menggunakan senjata yang dapat menyebabkan luka yang berlebihan pada korban dan cenderung menyiksa korban, lalu tidak boleh menggunakan metode yang akan berimbas pada kerusakan lingkungan hidup.

Pasal selanjutnya yang mengatur mengenai penggunaan senjata dalam peperangan menurut Protokol I/1977 adalah di Pasal 36.[38] Pada pasal tersebut disebutkan mengenai adanya kemungkinan penggunaan senjata baru namun harus tetap memperhatikan aturan dalam protokol ini serta tidak diperbolehkan menggunakan senjata dengan taktik berpura-pura melakukan sesuatu namun berujung pada pengkhianatan, contohnya melakukan negosiasi namun ternyata negosiasi tersebut hanya bersifat mengelabuhi saja.

Aturan pembatasan senjata lainnya dalam hukum humaniter selain diatur dalam konvensi di atas juga diatur pada beberapa konvensi lainnya. Meskipun konvensi ini tidak sebesar kedua konvensi sebelumnya, namun materi yang disajikan memiliki kesamaan dengan kedua konvensi sebelumnya, berikut adalah uraiannya:

a. Konvensi *Non-Proliferation Treaty* 1970

Konvensi ini berisi mengenai pembatasan penggunaan senjata nuklir. Dalam konvensi tersebut secara garis besar memiliki isi mengenai, *"non-proliferation, disarmament, and the right to use nuclear technology for good peace."*.[39] Artinya pada Konvensi ini berkaitan dengan penggunaan senjata nuklir yang dilarang, nuklir dilarang untuk digunakan dalam peperangan antar negara karena daya ledak dari nuklik ini tidak hanya menghasilkan panas atau energi yang luar biasa namun juga menghasilkan radiasi yang kuat dan dampaknya berkepanjangan. Radiasi dari nuklir ini akan merusak lingkungan, sumber daya alam, dan juga ekosistem di wilayah yang terdampak.[40]

Contoh nyata betapa jahatnya senjata nuklir adalah pada peristiwa Hiroshima dan Nagasaki serta di Chernobyl, dimana daerah-daerah tersebut hingga saat ini masih terdampak radiasi dari senjata nuklir, tanah yang dahulu subur berubah menjadi zat mati dan tidak dapat tumbuh dengan baik.

b. Konvensi Senjata Konvensional Tertentu

---

[36] Mohd Akram, *International Humanitarian Law Hague and Geneva Conventions on War Crimes, War Victims and Prisoners of War* (Selangor: International Law Book Services, 2005), halaman 100.
[37] Pasal 35 Protokol I Tahun 1977
[38] Pasal 36 Protokol I Tahun 1977
[39] Budi Pramono, *Hukum Humaniter* (Surabaya: Scopindo Media Pustaka, 2022), halaman 31.
[40] *Ibid.*

Konvensi lainnya adalah Konvensi Senjata Konvensional tertentu yang kerap disebut pula dengan Konvensi 1980 atau *Convention On Prohibitions Or Restrictions On The Use Of Certain Conventional Weapons Which May Be Deemed To Be Excessively Injurious Or To Have Indiscriminate Effects* (Konvensi CGW). Pada konvensi ini mengatur beberapa material yang tidak boleh dipergunakan selama peperangan berlangsung seperti pecahan yang tidak terdeteksi, ranjau anti kendaraan, perangkap tersembunyi, dan senjata bakar, senjata laser yang dapat membutakan pihak lawan. Masih adalagi beberapa aturan terkait yang mengatur beberapa senjata yang dilarang termasuk senjata kimia.[41]

Pada konvensi ini secara garis besar juga membedakan mengenai senjata otonom dan non otonom. Di mana senjata otonom merupakan senjata yang telah diaktifkan dan dapat memilih sasaran tanpa campur tangan manusia seperti penggunaan senjata laser, ranjau otomatis dan sebagainya sedangkan senjata non otonom adalah senjata yang masih membutuhkan campur tangan manusia untuk menjalankan senjata tersebut. [42]

Berkaitan dengan uraian konvensi yang mengatur tentang pembatasan penggunaan senjata dalam peperangan tersebut, hal ini penting untuk dilakukan sebab jika tidak diatur mengenai pembatasannya maka dapat dipastikan negara-negara yang berkonflik akan menggunakan seluruh jenis senjata pemusnah massal tanpa terkendali. Akibatnya dampak kerusakan dan kematian yang diciptakan akan lebih besar dan yang terdampak bisa saja tidak hanya kedua negara yang berkonflik namun juga seluruh negara di dunia.

2. Penggunaan *Cyberwarfare* sebagai Senjata Dalam Konflik Bersenjata

Cyberwarfare dapat diartikan bahwa *cyberwarfare* merupakan bagian dari serangan siber, namun dalam *cyberwarfare* terapat tiga unsur utama yang menjadi ciri khas dari tindakan cyberwarfare yang membedakannya dengan serangan siber lainnya, yaitu:[43]

a. Unsur Tindakan Militer

Serangan *cyberwarfare* merupakan bagian dari serangan militer yang dilakukan oleh negara yang saling berkonflik untuk saling menyerang dan melemahkan lawan dengan menggunakan cara “halus” bukan seperti serangan militer pada umumnya yang menggunakan ledakan atau tembakan. Serangan militer ini menggunakan atau memanfaatkan teknologi informasi dan komunikasi untuk melancarkan serangan tersebut sebagai serangan yang tidak terlihat.

b. Unsur Merusak Informasi bahkan Reputasi dari Negara Lawan

Dalam serangan *cyberwarfare*, tujuan utama yang dituju adalah menyerang negara lawan dengan mendapatkan berbagai informasi rahasia milik negara tersebut yang nantinya informasi tersebut akan dimanfaatkan untuk merusak reputasi negara lawan. Maksudnya adalah jika informasi rahasia milik suatu

[41] *Ibid.*
[42] *Ibid.*
[43] Suharto, Op.Cit, halaman 104.”

negara tersebar dan dipegang oleh pihak lawan, maka tentunya pihak lawan akan memanfaatkanny sebagai senjata untuk melawan negara tersebut tanpa harus menggunakan senjata api atau bom pada umumnya.

c. Unsur Untuk Memenangi Peperangan antar Negara

Terjadinya *cyberwarfare* memiliki tujuan utama untuk memenangkan peperangan atau konflik antar negara. Sehingga adanya tujuan ini yang kemudian membuat masing-masing negara akan saling melakukan serangan dengan menggunakan media teknologi informasi.

Ketiga unsur tersebut adalah hal yang membedakan *cyberwarfare* dengan serangan siber lainnya, umumnya serangan siber yang terjadi berkaitan dengan ranah tindakan pidana seperti pencurian data nasabah dan bersifat individual serta serangannya biasanya bersifat satu arah karena tidak ada perlawanan dari pihak korban, bukan seperti *cyberwarfare* yang melibatkan antar negara dan di dalamnya terjadi peperangan artinya ada perlawanan dari kedua negara.

Dasar kemunculan dari cyberwarfare sendiri didasarkan pada T*allinn Manual on the International Law Applicable to Cyber Warfare* ("*Tallinn Manual* 1.0") pada tahun 2013. *Tallinn Manual* merupakan murni pendapat dari kelompok ahli, tidak bersifat mengikat dan bukan merupakan pernyataan/doktrin dari NATO, negara donatur maupun organisasi manapun. *Tallinn Manual* merupakan sumber hukum internasional sebagai *public conscience* yakni sebagai celah penutup kekosongan hukum dan memberikan kepastian hukum mengenai *cyberwarfare*.

Kemunculan serangan *cyberwarfare* yang saat ini tengah menjadi tren juga merupakan bentuk pengaplikasian dari Pasal 36 Protokol I/1977 yang menyebutkan bahwa:

In research, development produce or obtain a weapon new, tools or methods of warfare, a The High Contracting Party is obliged to determine whether under certain circumstances or all circumstances its use will not be prohibited by this Protocol or by any regulations other than applicable international law towards the High Contracting Party.

Pasal tersebut dapat diartikan bahwa seiring berkembangnya waktu, dunia mengalami perubahan yang terus berjalan. Hal ini yang juga terjadi pada dunia peperangan di mana tidak menutup kemungkinan bahwa suatu hari nanti akan bermunculan senjata-senjata baru yang digunakan dalam berperang dan menurut peneliti *Cyberwarfare* saat ini tengah menjadi bagian dari senjata baru tersebut yang tercipta karena adanya perkembangan teknologi yang cukup luar biasa dan berlangsung cepat.

Cyberwarfare menurut pendapat peneliti, telah berkembang menjadi perang modern yang juga mendapatkan perhatian mendalam dari negara-negara terutama yang sedang terlibat konflik. Hal ini disebabkan meskipun perang ini terjadi di dunia maya, namun perang ini sama halnya seperti menjaga kedaulatan negara dari sisi darat, udara, laut, dan ruang angka. Dunia maya ditempatkan sebagai matra kelima dalam medan perang, karena kedaulatan negara saat ini juga terdapat pada dunia maya.

Jenis senjata utama dalam *cyberwarfare* adalah *software Malware* yang bersifat merusak dan mengganggu fungsi dari komputer dan aplikasi lainnya yang berbasis internet. *Cyberwarfare* saat ini menjadi alat pelumpuh utama bagi negara lawan yang ingin mengalahkan negara lainnya. Cara kerjanya adalah ketika sistem suatu negara berhasil dilumpuhkan oleh virus *Malware* dimana virus ini benar-benar bersifat merusak dan mengunci sistem yang berhasil diambil alih, biasanya virus ini akan mengunci data penting dari korban. Ketika data penting kenegaraan berhasil dikuncil dan diambil alih, maka pihak yang berhasil mengambil alih tersebut akan meminta tebusan atau transaksi timbal balik kepada negara yang menjadi korban. Transaksi inilah yang diharapkan oleh negara lawan untuk meminta beberapa hal yang diinginkannya dalam peperangan tersebut.[44]

Peneliti berpendapat bahwa dampak yang ditimbulkan *cyberwarfare* tersebut jika diteliti lebih lanjut jauh lebih berbahaya daripada kontak senjata, karena pihak negara yang mengalami serangan siber tidak mempunyai pilihan lain selain menyerah atau menuruti kemamuan negara lawan karena ada sandera yang harus dibebaskan yakni terkait sistem keamanan dan pertahanan negara.

3. Aturan Penggunaan *Cyberwarfare* dalam Konflik Bersenjata Menurut Pandangan Hukum Humaniter Internasional

Aturan mengenai penggunaan *cyberwarfare* dapat dikaitkan dengan beberapa konvensi yang secara khusus mengatur tentang pelarangan penggunaan senjata. Berikut adalah beberapa aturan HHI yang dapat dikaitkan dengan penggunaan *Cyberwarfare* dalam peperangan:[45]

a. Konvensi Den Haag

Aturan dalam konvensi tersebut dapat diterapkan dalam penggunaan *cyberwarfare* , hal ini didasarkan pada bunyi Pasal 24 Konvensi IV Den Haag 1907 yang dalam salah satu kalimatnya mengatur tentang "penyerangan atau pemboman dengan alat apapun…." Kata alat apapun disini dapat dikembangkan menjadi alat perang lain yang terus bermunculan seiring waktu, salah satunya *cyberwarfare.*

b. Konvensi Jenewa 1949

Pasal 27 dan Pasal 31 ini dapat diterapkan pada penggunaan serangan siber dalam *cyberwarfare* sebagai senjata perang. Artinya serangan *cyberwarfare* yang dilakukan tidak boleh menyerang pribadi warga sipil yang berpotensi melanggar hak dari warga sipil untuk memperoleh privasi dan keamanan diri sendiri. Selain itu *cyberwarfare* juga tidak boleh menahan diri pribadi dari warga negara seperti contoh melakukan serangan terhadap data pribadi warga negara, yang digunakan untuk memaksa negara lawan menyerah dengan menggunakan paksaan moral kepada warga negara.

---

[44] Maskun, *Korelasi Kejahatan Siber Dan Kejahatan Agresi Dalam Hukum Internasional* (Makassar: Nas Media Indonesia, 2018), halaman 50.
[45] *Ibid.*

c. Protokol I 1977

Pada Pasal 36 protokol ini diatur bahwa dimungkinkan adanya kemunculan senjata baru dalam berperang hal ini yang terjadi dengan kemunculan *cyberwarfare* namun perlu diperhatikan bahwa serangan siber tersebut tidak diperkenankan menyerang sektor-sektor penting yang dapat berimbas pada kelangsungan hidup warga sipil.

B. Pertanggungjawaban hukum terhadap Rusia yang telah melakukan *cyber warfare* dalam konflik bersenjata dengan Ukraina

1. Penggunaan *Cyberwarfare* oleh Rusia maupun Ukraina dalam Konflik Bersenjata antar Kedua Negara

Penggunaan serangan siber dalam *cyberwarfare* yang dilakukan oleh Rusia bukanlah yang pertama kali dilakukan, dahulu saat berperang dengan Georgia, Rusia telah menggunakan serangan berbasis siber. Hal ini yang kemudian dilakukan kembali saat Rusia berperang melawan Ukraina. Rusia berkali-kali diduga melakukan serangan siber dengan melakukan serangan Ddos dengan Ukraina, *ransomware NotPetya*, hingga kampanye *Phising*.[46]

Berikut adalah contoh peristiwa penggunaan *cyberwarfare* yang terjadi selama perang antara Rusia dengan Ukraina: [47]

a. Pada tahun 2014, Rusia melakukan serangan dengan menggunakan DdoS, serangan ini memiliki kekuatan 32 kali lebih mengerikan dibandingkan dengan serangan *cyberwarfare* lainnya. Serangan ini dilakukan selama 8 menit saja namun dampaknya cukup terasa karena akhirnya mengacaukan jaringan komputer dan komunikasi di negara Ukraina. Cara ini dilakukan sebagai pengalihan kedatangan Rusia di Krimea.
b. Pada tahun yang sama pula Rusia juga melakukan *cyberwarfare* dengan melumpuhkan sistem Komisi Pemilihan Umum Ukraina pada 3 hari sebelum pemilihan Presiden Ukraina dimulai. Serangan yang dilakukan tersebut memiliki tujuan untuk menciptakan kekacauan dan membantu kandidat pro-Rusia untuk meraih kemenangannya;
c. Pada tahun 2016, Rusia kembali melakukan *cyberwarfare* dengan melakukan serangan terhadap jaringan pasokan listrik Ukraina. Akibat dari adanya serangan terhadap sektor kelistrikan tersebut membuat kehidupan masyarakat Ukraina menjadi terganggu.
d. Rusia melakukan serangan *cyberwarfare* terhadap sistem perbankan Ukraina, yang menyebabkan bank Ukraina seperti Bank Nadra, Oschad Bank, dan juga Privat Bank. Serangan tersebut dilakukan dengan menggunakan *Malware BlackEnergy*, dimana malware jenis ini secara khusus menyerang jaringan bidang perbankan. Serangan di bidang keuangan ini dilakukan Rusia dengan tujuan Rusia dapat memperoleh identitas dan melakukan rekayasa finansial

[46] Wasis Susetio, "Perang Rusia-Ukraina : Mencari Keseimbangan Dunia Baru," *Jurnal Abdimas* vol. 8, no. 5 (2022), halaman 334.
[47] *Ibid.*

termasuk memindahkan dana ke rekening yang telah dikontrol oleh Rusia tersebut.

Serangan *cyberwarfare* Rusia pada Ukraina tersebut tidak hanya sebatas pada kedua peristiwa tersebut, sebab Rusia telah bersiap dalam berkonflik dalam dunia maya atau *cyberwarfare*. Puncaknya di tahun 2021 yang lalu, Rusia melalui pihak teknologi yang dimiliknya, secara sporadis menargetkan *cyberwarfare* pada Ukraina termasuk organisasi maupun negara lainnya yang secara terang-terangan turut membela Ukraina. Serangan *cyberwarfare* yang dilakukan salah satunya dengan menyerang ratusan sistem di pemerintahan Ukraina sengan menggunakan serangan virus *Malware Wiper*. Serangan ini telah menyerang sistem pemerintahan, teknologi informasi, energi, dan organisasi keuangan pada serangan *cyberwalfare* tersebut. [48]

Salah satu akibat yang ditimbulkan akibat penggunaan serangan *cyberwarfare* dalam peristiwa Rusia dan Ukraina tersebut adalah masyarakat tidak dapat melakukan akses terhadap layanan publik di Ukraina sehingga seluruh aktivitas di negara tersebut lumpuh. Rusia dalam melakukan *cyberwarfare* tersebut dibantu oleh *Advanced President Threat* (APT) yang juga menargetkan Ukraina. APT merupakan *campaign* serangan yang melakukan aksinya secara senyap dengan jangka waktu relatif panjang dengan melakukan beragam serangan pada *cyberwarfare* yang bertujuan untuk memperoleh informasi maupun data sensitif tingkat tinggi.[49]

APT merupakan ancaman yang melakukan serangan secara terstruktur, terencana, dan dilakukan dalam jangka waktu yang cukup lama yang dilakukan oleh organisasi baik yang berasal dari pemerintahan suatu negara, maupun non pemerintahan termasuk juga komunitas tertentu. APT telah menjalin relasi dengan pemerintahan Rusia dalam melakukan invasi secara siber melalui *cyberwarfare*. Hal ini dibuktikan dengan adanya kerjasama antara APT dengan beberapa organisasi intelijen milik pemerintahan Rusia.[50]

Serangan *cyberwarfare* yang terjadi tidak hanya dilakukan oleh pihak Rusia saja, namun pihak Ukraina juga berupaya melakukan serangan balasan melalui dunia siber terhadap Rusia dengan cara mengundang para hacker *undergorund* untuk mengantisipasi serangan IT yang dilakukan oleh Rusia dan juga sekaligus pemerintah Ukraina membentuk tim IT untuk mengintai pasukan Rusia melalui dunia maya. Pihak pemerintah Ukraina melalui tim IT tersebut telah beberapa kali melakukan serangan siber pada situs pemerintahan dan bank Rusia serta mengganti konten-konten tertentu dengan gambar kekerasan perang. Meskipun pihak Ukraina juga melakukan serangan *cyberwarfare* namun intensitasnya tidak sebanyak pihak Rusia.[51]

Berdasarkan uraian tersebut maka dapat diartikan bahwa dalam peperangan yang terjadi antara Rusia dan Ukraina telah dilakukan dengan menggunakan

---

[48] *Ibid.*
[49] *Ibid.*
[50] *Ibid.*
[51] Roy, "Bukan Dunia Nyata, Perang Rusia-Ukraina Ngeri Di Dunia Maya," 2024, https://www.cnbcindonesia.com/tech/20220303100401-37-319748/bukan-dunia-nyata-perang-rusia-ukraina-ngeri-di-dunia-maya, diakses tanggal 29 Februari 2024.

cyberwarfare . Serangan ini tidak hanya terjadi satu atau dua kali saja namun beberapa kali dilakukan oleh Rusia untuk menyerang Ukraina begitu pula sebaliknya Ukraina menyerang Rusia menggunakan *cyberwarfare* namun dengan intensitas yang lebih sedikit dibanding Rusia. Rusia dan Ukraina melakukan *cyberwarfare* dengan menargetkan sejumlah fasilitas penting di negara lawan mulai dari listrik hingga perbankan dan sekaligus digunakan untuk men-*distract* Ukraina ketika Rusia memasuki wilayah Krimea.

2. Pertanggungjawaban Hukum Terhadap Rusia yang Melakukan *Cyberwarfare* dalam Konflik dengan Ukraina

Cyberwarfare merupakan salah satu jenis senjata peperangan yang seharusnya sudah dilakukan pelarangan seperti beberapa jenis senjata lain yang diatur dalam HHI, sebab dampak yang ditimbulkan juga cukup membahayakan seperti yang telah diuraikan sebelumnya. Rusia sebagai pihak yang melakukan *cyberwarfare* hingga berdampak bagi warga sipil Ukraina sepatutnya harus mempertanggung jawabkan perbuatannya berkaitan dengan tanggung jawab negara.

Bentuk pertanggungjawaban yang dapat dilakukan Rusia juga berkaitan dengan kewenangan dari *International Court of Justice* (ICJ) dalam hal ini pihak Ukraina yang merasa dirugikan akibat perbuatan dari Rusia dapat melaporkan tindakan Rusia tersebut pada ICJ atas invasi Rusia dalam bentuk *cyberwarfare* yang berdampak cukup panjang bagi warga sipil Ukraina. Tindakan yang dilakukan Rusia juga dapat dikaitkan dengan pelanggaran terhadap Hak Asasi Manusia, karena tindakan *cyberwarfare* tersebut sedikit banyak telah memepengaruhi hak hidup masyarakat terutama hak untuk bebas hak untuk hidup dengan baik termasuk pemenuhan kesehatan.

Pemberian sanksi selain didasarkan pada pelaporan pada ICJ juga dapat dilakukan oleh negara-negara lain di luar Ukraina dan Rusia. Namun pemberian sanksi ini memiliki perbedaan dibandingkan pemberian sanksi ICJ, negara-negara lain selain Rusia dan Ukraina dapat memberikan sanksi lebih kepada sanksi terkait hubungan kenegaraan. Dasar hukum dari pemberian sanksi ini berkaitan dengan konvensi-konvensi yang telah disepakati bersama terutama dalam kasus ini adalah mengenai konvensi pembatasan penggunaan senjata.

Pihak Rusia juga dapat menerima pertanggungjawaban dari sanksi-sanksi yang diberikan oleh negara-negara lain di luar Ukraina dan Rusia. Selain berdasarkan pelaporan pada ICJ, negara-negara ini turut memberikan hukuman sebab apa yang telah dilakukan oleh Rusia telah melanggar aturan dalam HHI ditambah tindakan tersebut telah melanggar hak asasi manusia. Bentuk sanksi yang diberikan oleh negara memiliki perbedaan ada yang berupa pencabutan hubungan bilateral, pelarangan ekspor-impor dalam bidang perdagangan antara Rusia dengan negara tujuan, dan sebagainya. Adanya sanksi dari negara lain ini semakin mengindikasikan bahwa Rusia telah melakukan pelanggaran terhadap HHI.

Contoh negara yang memberikan sanksi kepada Rusia adalah Uni Eropa, sanksi tersebut dilakukan dengan tujuan untuk memukul mundur sekto keuangan, energi dan juga transportasi Rusia termasuk kontrol ekspor dan larangan

pembmiayaan perdagangan. Negara lainnya yang turut memberi sanksi adalah Selandia Baru yang melarang ekspor barang ke militer Rusia dan pasukan keamanan. Bahkan negara Amerika Serikat juga turut memberikan sanksi yakni dengan melakukan blok terhadap ekspor dan teknologi kepada Rusia.[52]

Berdasarkan uraian tersebut, dapat diartikan bahwa Rusia telah memenuhi unsur dalam *state responsibility* dan perbuatannya telah melanggar segala ketentuan dalam HHI termasuk prinsip HHI yang harus dilakukan pemisahan terhadap pihak yang boleh dilakukan serangan dan tidak boleh diserang. Oleh sebab itu sebagai bentuk pertanggungjawaban negara, pihak Rusia harus dibebankan sanksi yang terdapat pada Konvensi Genewa 1949 dan Konvensi Den Haag berkaitan dengan penggunaan senjata dan pelanggaran terhadap prinsip HHI.

Dalam Konvensi Jenewa 1949 disebutkan bahwa dasar pertanggungjawaban suatu negara terkait dengan kejahatan internasional adalah apabila melakukan beberapa tindakan berikut yaitu pembunuhan yang dilakukan secara sengaja, penyiksaan atau perlakuan tidak manusiawi, penghancuran dan perampasan properti secara berlebihan, dan penyanderaan. Berdasarkan permasalahan yang dilakukan pihak Rusia dapat diduga bahwa Rusia telah melakukan beberapa tindakan yang menjadi indikator pelanggaran Konvensi Jenewa tersebut yakni pembunuhan yang sengaja terhadap warga sipil dan militer di negara lawan secara berlebihan ditambah penyanderaan dan penyiksaan yang tidak manusiawi. Hal inilah yang menjadi dasar pertanggungjawaban Rusia berdasarkan Konvensi Jenewa 1949.

Negara yang melakukan pelanggaran perang seperti yang dilakukan oleh Rusia terhadap Ukraina maka sebagai bentuk pertanggungjawaban, kasus ini bisa dilimpahkan ke pengadilan internasional. Mahkamah Internasional di bawah Perserikatan Bangsa-Bangsa (PBB) terbagi menjadi dua jenis, yaitu Mahkamah Internasional (ICJ) yang mempunyai fungsi mengadili dan menyelesaikan perselisihan antar negara yang tergabung dalam Perserikatan Bangsa-Bangsa, sedangkan Mahkamah Pidana Internasional Court (ICC) yang Berdasarkan Statuta Roma tahun 1998 merupakan lembaga peradilan internasional yang hadir untuk mengadili kejahatan luar biasa yang dilakukan oleh individu dalam suatu negara, kejahatan tersebut terdiri dari kejahatan genosida, kejahatan terhadap kemanusiaan, kejahatan perang, kejahatan agresi.

Dalam kasus yang terjadi terkait dengan penyerangan Rusia kepada Ukraina, secara yurisdiksi tidak dapat diselesaikan melalui ICC karena baik Ukraina maupun Rusia bukanlah negara anggota yang meratifikasi Statuta Roma tahun 1998 sebagai dasar penetapan lahirnya ICC. Perkara yang dapat ditangani oleh ICC apabila dalam keadaan sebagai berikut:

a. Hanya untuk negara-negara anggota yang meratifikasi Statuta Roma 1998 atau
b. Dalam hal pelaku kejahatan berasal dari suatu negara yang bukan anggota ratifikasi tetapi korban kejahatannya berasal dari negara anggota, hal ini tetap menjadi jurisdiksi ICC.

---

[52] Taufik Purbo Satrio, "Perintah Penangkapan Vladimir Putin Oleh Pengadilan Pidana Internasional Dalam Perspektif Hukum Internasional," *Jurnal Pembangunan Hukum Indonesia* vol. 5, no. 3 (2023), halaman 457.

Oleh karena itu, baik Ukraina maupun Rusia tidak meratifikasi Statuta Roma sehingga keduanya bukan negara yang mematuhi Statuta Roma, sehingga permasalahan tersebut dapat ditangani oleh ICJ yang memiliki yurisdiksi untuk menyelesaikan permasalahan yang terjadi antara Rusia dan Ukraina, yang keduanya juga merupakan anggota PBB. Namun apabila ICJ juga tidak membuahkan hasil, maka Dewan Keamanan PBB dapat membuat resolusi/rujukan agar permasalahan antara Rusia dan Ukraina, khususnya terkait kejahatan perang, dapat diselesaikan dalam yurisdiksi ICC.

Rusia dapat dibebankan pertanggungjawaban melalui ICJ dengan mekanisme yang diawali adanya pengaduan dari beberapa negara terkait dengan tindakan Rusia atas Ukraina. Proses investigasi ini dilakukan setelah ICJ mendapati adanya pengaduan dari beberapa negara terhadap adanya dugaan kejahatan perang, kejahatan kemanusiaan yang dilakukan oleh Rusia. Selanjutnya pihak ICJ dapat melakukan penangkapan kepada Vladimir Putin selaku Presiden Rusia yang didasarkan pada adanya dugaan pelanggaran kejahatan perang dalam Konvensi Jenewa 1949 dan pada tanggal 17 Maret 2023 telah dilayangkan surat penangkapan kepada Vladimir Putin.

Vladimir Putin meskipun telah diberikan surat penangkapan namun dirinya menolak untuk ditangkap karena merasa memiliki kekebalan hukum berkaitan dengan Rusia yang tidak melakukan ratifikasi Statuta Roma. Meskipun demikian, sepatutnya penangkapan terhadap Vladimir Putin tetap dapat dilakukan dengan dasar Pasal 27 ayat (2) Piagam PBB yang menyebutkan, *"Immunities or special procedural rules which may attach to the official capacity of a person, where under national law or international law, shall not bar the Court from exercising its jurisdiction over such a person"* Artinya bahwa posisi dan imunitas yang melekat pada kepala negara tidak menjadi hambatan bagi Mahkamah Internasional untuk memulai proses pemeriksaan hingga penjatuhan sanksi pidana terhadap kepala negara tersebut.

Rusia meskipun tidak meratifikasi Statuta Roma namun Rusia merupakan bagian dari anggota PBB sehingga ketentuan dalam Piagam PBB ini dapat menjadi dasar untuk melakukan penangkapan dan pemrosesan Vladimir Putin selaku kepala negara Rusia dalam tahapan selanjutnya karena adanya dugaan kejahatan perang yang telah dilakukan Rusia kepada Ukraina.

IV. SIMPULAN

Pengaturan tentang *Cyberwarfare* dalam konflik bersenjata menurut Hukum Humaniter Internasional didasarkan pada Pasal 22 dan Pasal 23 Konvensi Den Haag 1907 yang mengatur tentang pembatasan penggunaan senjata dalam peperangan atau konflik bersenjata. Selain itu dasar hukum lainnya ada di Pasal 35 Protokol I/1977 mengenai aturan kebebasan bagi masing-masing negara untuk memilih senjata perang namun tetap terbatas serta Pasal 36 Protokol I/1977 mengenai jenis alat perang metode baru. Dasar hukum lainnya ada di Konvensi Senjata Konvensional Tertentu yang membedakan senjata otonom dan non otonom. Kemudian seiring berkembangnya waktu perihal *cyberwarfare* mengacu pada Konvensi Budapest yang mengatur tentang kejahatan siber dan terakhir terkait dengan *Tallinn Manual on the International Law Applicable to Cyber*

Warfare ("*Tallinn Manual* 1.0") pada tahun 2013 di mana *Tallinn Manual* merupakan murni pendapat dari kelompok ahli, tidak bersifat mengikat dan bukan merupakan pernyataan/doktrin dari NATO, negara donatur maupun organisasi manapun. *Tallinn Manual* merupakan sumber hukum internasional sebagai *public conscience* yakni sebagai celah penutup kekosongan hukum dan memberikan kepastian hukum mengenai *cyberwarfare* terutama di Pasal 43 *Tallinn Manual* 1.0.

Pertanggungjwaban hukum terhadap Rusia yang telah melakukan serangan *Cyberwarfare* dalam konflik bersenjata dengan Ukraina didasarkan pada Konvensi Jenewa 1949 di mana Rusia sebagai anggota PBB telah meratifikasi konvensi ini. Tindakan yang dilakukan oleh Rusia diduga merupakan kejahatan perang dan hal ini telah melanggar Pasal 144 Konvensi Jenewa IV Tahun 1949 di mana negara-negara yang meratifikasi konvensi ini wajib mematuhi segala ketentuan di dalamnya dan menerapkannya dalam kehidupan negara namun Rusia tidak melakukan hal tersebut dan tindakan Rusia ini termasuk pelanggaran berat seperti yang ditentukan di Pasal 147 Konvensi Jenewa IV 1949 seperti pembunuhan disengaja, penganiayaan tidak berperikemanusiaan, penderitaan berkepanjangan dan sebagainya. Pelanggaran lainnya termasuk melanggar Konvensi Den Haag di Pasal 22 dan Pasal 23 tentang penggunaan senjata yang mengakibatkan penderitaan yang berkepanjangan. Oleh sebab itu terhadap Rusia dapat dikenakan pertanggungjawaban yang ditangani oleh Mahkamah Internasional. Namun dalam kasus yang terjadi terkait dengan penyerangan Rusia kepada Ukraina, secara yurisdiksi tidak dapat diselesaikan melalui ICC karena baik Ukraina maupun Rusia bukanlah negara anggota yang meratifikasi Statuta Roma tahun 1998 sebagai dasar penetapan lahirnya ICC, oleh karena itu, permasalahan tersebut dapat ditangani oleh ICJ yang memiliki yurisdiksi untuk menyelesaikan permasalahan yang terjadi antara Rusia dan Ukraina, yang keduanya juga merupakan anggota PBB. Namun apabila ICJ juga tidak membuahkan hasil, maka Dewan Keamanan PBB dapat membuat resolusi/rujukan agar permasalahan antara Rusia dan Ukraina, khususnya terkait kejahatan perang, dapat diselesaikan dalam yurisdiksi ICC.

DAFTAR PUSTAKA

A. Buku

Akram, Mohd. *International Humanitarian Law Hague and Geneva Conventions on War Crimes, War Victims and Prisoners of War*. Selangor: International Law Book Services, 2005.

Andrew D. Murray. *The Regulation of Cyberspace: Control in The Online Environment*. Abingdon: Routledge-Cavendish, 2007.

Gulo, W. *Metodologi Penelitian*. Jakarta: Grasindo, 2019.

Haryomataram. *Hukum Humaniter*. Jakarat: Rajawali Press, 1984.

———. *Pengantar Hukum Humaniter*. Jakarta: Rajawali Press, 1994.

Herman Suryokumoro. *Hukum Humaniter Internasional: Kajian Norma Dan Kasus*. Malang: Brawijaya University Press, 2020.

Kurnia, Erwin. *Kebijakan Straegi Keamanan Cyber Nasional Dalam Menghadapi Perang Cyber (Cyber Warfare)*. Jakarta: Universitas Pertahanan Indonesia, 2014.

Margarita Levin Jaitner. *Cyber War in Perspective: Russian Aggression Against Ukraine*. Tallin: CEO Publications, 2015.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group, 2013.

Maskun. *Korelasi Kejahatan Siber Dan Kejahatan Agresi Dalam Hukum Internasional*. Makassar: Nas Media Indonesia, 2018.

Pramono, Budi. *Hukum Humaniter*. Surabaya: Scopindo Media Pustaka, 2022.

Qamar, Nurul. *Metode Penelitian Hukum*. Makassar: Social Politics Genius, 2017.

Qutub, Sayid. *Cyber Terrorism Dalam Hukum Islam*. Jakarta: Irama Offset, 2015.

Richard Clarke dan Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Harper Collins Publishers, 2010.

Rukhmana, Trisna. *Metode Penelitian Kualitatif*. Batam: Rey Media Grafika, 2022.

Saebani, Beni Ahmad. *Metode Penelitian Kualitatif*. Bandung: Pustaka Setia, 2019.

Steve Winterfeld. *The Basic of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Amsterdam: Syngress, 2013.

Sunggono, Bambang. *Metodologi Penelitian Hukum*. Jakarta: Raja Grafindo, 2017.

Syahrum, Muhammad. *Pengantar Metodologi Penelitian Hukum*. Riau: Dotplus Publisher, 2022.

Wagiman, Anasthasya, dan Saartje Mandagi. *Terminologi Hukum Internasional*. Jakarta: Sinar Grafika, 2016.

Wahyu Wagiman. *Hukum Humaniter Dan HAM*. Jakarta: : Lembaga Studi dan Advokasi Masyarakat, 2005.

B. Jurnal

Azhar Unwala dan Shaheen Gori. "Brandishing the Cybered Bear: Information War and Russian-Ukraine Conflict." *Military Cyber Affairs* 1, no. 1 (2015): 7.

Esbjorn Rosenbland dalam Rafika Mayasari Siregar. "Tinjauan Yuridis Konvensi Jenewa IV Tahun 1949 Terhadap Negara-Negara Yang Berperang Menurut Hukum Internasional." *Sumatra Journal of International Law*, 2013, 7.

I. Gst Ngr Hady Purnama Putera. "Penggunaan Exoskeleton Sebagai Senjata Dalam Konflik Bersenjata Internasional Di Masa Yang Akan Datang Ditinja Dari Prinsip-Prinsip Hukum Humaniter Internasional." *Jurnal Komunikasi Hukum* 2, no. 2 (2016): 185.

———. "The Evolution of Warfare." *International Review of The Red Cross* 97, no. 900 (2015): 1473.

Jean Pictet. "The Fundamental Principles of the Red Cross: Commentary." *International Review of The Red Cross* 19, no. 210 (1979): 6.

Raka Permana Nayaspoetra, Joko Setiyono dan Nuswantoro Dwiwarno. "Perlindungan Objek Sipil Atas Penggunaan Cyber Warfare Dalam Konflik Bersenjata Antara Rusia Dengan Ukraina Dalam Perspektif Hukum Humaniter Internasional." *Diponegoro Law Journal*, 2019, 1.

Suharto, Miko Aditiya. "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional." *Jurnal Risalah Hukum* 17, no. 2 (2021): 98–107.

Susetio, Wasis. "Perang Rusia-Ukraina : Mencari Keseimbangan Dunia Baru." *Jurnal Abdimas* 8, no. 5 (2022): 334.

Taufik Purbo Satrio. "Perintah Penangkapan Vladimir Putin Oleh Pengadilan Pidana Internasional Dalam Perspektif Hukum Internasional." *Jurnal Pembangunan Hukum Indonesia* 5, no. 3 (2023): 457.

Vincent Bernard. "Tactics, Techniques, Tragedies: A Humanitarian Perspective on Thr Changing Face to War." *International Review of The Red Cross* 97, no. 900 (2015): 959–68.

Yohana Tri Meiliyani, Joko Setiyono, dan Kabul Supriyadhie. "Kajian Hukum Humaniter Internasional Mengenai Cyber Warfare Dalam Konflik Bersenjata Internasional Antara Israel Dan Palestina Atas Gaza." *Diponegoro Law Journal* 8, no. 2 (2018): 1598

C. Internet

ICRC. "Rule 14 Proportionality in Attack," 2022. https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule14.

Joshua Davis. "Hackers Take Down the Most Wired Country in Europe," 2022. http://www.wired.com/2007/08/ff-estonia/.

Markoff, John. "Before the Gunfire, Cyberattacks," 2022. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

Roy. "Bukan Dunia Nyata, Perang Rusia-Ukraina Ngeri Di Dunia Maya," 2024. https://www.cnbcindonesia.com/tech/20220303100401-37-319748/bukan-dunia-nyata-perang-rusia-ukraina-ngeri-di-dunia-maya.

Tom Urent, Bart Hagoyen dan Fergus Hanson. "Defining Offensive Cyber Capabilities," 2022. https://www.aspi.org.au/report/defining-offensive-cyber-capabilities.