UNIVERSITAS KATOLIK PARAHYANGAN
FAKULTAS HUKUM

Terakreditasi Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi *Nomor: 2193/SK/BAN-PT/AK-ISK/S/IV/2022*

URGENSI PEMBENTUKAN INSTRUMEN HUKUM HUMANITER INTERNASIONAL TENTANG *CYBER WARFARE*

OLEH:

Stephanie Liestia Gunawan
NPM: 6052001306

PEMBIMBING
Adrianus Adityo Vito Ramon, S.H., LL.M. (adv.)

Penulisan Hukum

Disusun Sebagai Salah Satu Kelengkapan
Untuk Menyelesaikan Program Pendidikan Sarjana
Program Studi Ilmu Hukum

2024

Penulisan Hukum dengan judul

Urgensi Pembentukan Instrumen Hukum Humaniter Internasional Tentang *Cyber Warfare*

yang ditulis oleh:

Nama : Stephanie Liestia Gunawan

NPM : 6052001306

Pada tanggal: 21/06/2024

Telah disidangkan pada

Ujian Penulisan Hukum Program Studi Hukum Program Sarjana

Fakultas Hukum Universitas Katolik Parahyangan

Pembimbing

Adrianus Adityo Vito Ramon, S.H., LL.M. (Adv.)

Pj Dekan,

Dr. R.B. Budi Prastowo, S.H., M.H.

PERNYATAAN INTEGRITAS AKADEMIK

Dalam rangka mewujudkan nilai-nilai ideal dan standar mutu akademik yang setinggi-tingginya, maka Saya, Mahasiswa Fakultas Hukum Universitas Katolik Parahyangan yang bertanda tangan di bawah ini :

Nama : **Stephanie Liestia Gunawan**

NPM : **6052001306**

Dengan ini menyatakan dengan penuh kejujuran dan dengan kesungguhan hati dan pikiran, bahwa karya ilmiah / karya penulisan hukum yang berjudul:

"Urgensi Pembentukan Instrumen Hukum Humaniter Internasional Tentang *Cyber Warfare*"

Adalah sungguh-sungguh merupakan karya ilmiah /Karya Penulisan Hukum yang telah saya susun dan selesaikan atas dasar upaya, kemampuan dan pengetahuan akademik Saya pribadi, dan sekurang-kurangnya tidak dibuat melalui dan atau mengandung hasil dari tindakan-tindakan yang:

a. Secara tidak jujur dan secara langsung atau tidak langsung melanggar hak-hak atas kekayaan intelektual orang lain, dan atau
b. Dari segi akademik dapat dianggap tidak jujur dan melanggar nilai-nilai integritas akademik dan itikad baik;

Seandainya di kemudian hari ternyata bahwa Saya telah menyalahi dan atau melanggar pernyataan Saya di atas, maka Saya sanggup untuk menerima akibat-akibat dan atau sanksi-sanksi sesuai dengan peraturan yang berlaku di lingkungan Universitas Katolik Parahyangan dan atau peraturan perundang-undangan yang berlaku.

Pernyataan ini Saya buat dengan penuh kesadaran dan kesukarelaan, tanpa paksaan dalam bentuk apapun juga.

Bandung, 5 juni 2024

Mahasiswa penyusun Karya Ilmiah/ Karya Penulisan Hukum

Stephanie Liestia Gunawan

6052001306

ABSTRAK

Cyber warfare merupakan sebuah metode yang mengacu pada penggunaan sarana dan metode siber militer dalam situasi konflik bersenjata di *cyberspace*. Meskipun, *cyber warfare* sendiri merupakan metode konflik bersenjata yang baru, tetapi hukum humaniter internasional tetap bisa diterapkan dalam konteks *cyber warfare*. Mengingat, hukum humaniter internasional dalam komentarnya tentang Pasal 36 Protokol Tambahan I Konvensi Jenewa Tahun 1977 mengakui adanya perkembangan metode dan cara negara dalam berkonflik (*means and methods of warfare*). Sebelum berbicara mengenai metode serangan, hal yang harus dilihat terlebih dahulu ialah apakah jenis serangan yang digunakan oleh *cyber warfare* dapat memenuhi istilah "serangan". Syarat utama yang harus dipenuhi dalam mengkategorikan sebuah serangan, ialah dampak yang ditimbulkan dari serangan tersebut. Jenis serangan yang ditimbulkan harus bisa menimbulkan dampak fisik terhadap obyek yang diserang. Masih terdapat perdebatan mengenai dampak yang ditimbulkan oleh *cyber warfare*, terutama jika serangan hanya memberikan dampak berupa kerusakan terhadap infrastruktur kritis. Sejauh ini, aplikasi hukum humaniter internasional mengenai *cyber warfare* sudah berusaha dilakukan oleh IGE dengan menerbitkan sebuah panduan yang diberi nama Manual Tallinn. Mengingat, panduan dalam Manual Tallinn bukan merupakan bagian dari sumber hukum internasional sehingga tidak memiliki kekuatan yang mengikat. Tujuan dari penelitian ini, ialah untuk menjelaskan mengenai urgensi bagi negara untuk membentuk sebuah aturan tentang *cyber warfare* yang memuat metode penyerangan, subyek, obyek, dan perlindungan terhadap masyarakat sipil serta infrastruktur sipil. Selain itu, penulis juga mencari urgensi dibalik pembentukan aturan hukum tersebut, seperti pemenuhan dampak fisik sebagai akibat dari serangan dan panduan Manual Tallinn yang berbentuk *soft law*. Penelitian ini dilakukan menggunakan Konvensi Jenewa serta aturan lainnya yang mengatur tentang konflik bersenjata. Didukung dengan sumber lainnya, seperti dokumen PBB dan sumber literatur buku, jurnal, serta artikel. Berdasarkan hasil penelitian yang didapat, masih terdapat urgensi bagi negara untuk membentuk hukum humaniter internasional mengenai *cyber warfare*.

Kata Kunci: Perang Siber, Hukum Humaniter Internasional, Serangan Jaringan Komputer

ABSTRACT

Cyber warfare is a method that refers to the use of military cyber means and methods in situations of armed conflict in cyberspace. Although, cyber warfare itself is a new method of armed conflict, international humanitarian law can still be applied in the context of cyber warfare. Given, international humanitarian law in its commentary on Article 36 of Additional Protocol I to the 1977 Geneva Conventions recognises the development of methods and means of warfare. Before talking about the method of attack, what must be seen first is whether the type of attack used by cyber warfare can fulfil the term "attack". The main requirement that must be met in categorising an attack is the impact caused by the attack. The type of attack must be able to cause physical impact on the object being attacked. There is still debate about the impact of cyber warfare, especially if the attack only causes damage to critical infrastructure. So far, the application of international humanitarian law regarding cyber warfare has been attempted by the IGE by publishing a guide called the Tallinn Manual. However, the guidelines in the Tallinn Manual are not part of the sources of international law so they do not have binding force. The purpose of this research is to explain the urgency for the state to establish a regulation on cyber warfare that contains methods of attack, subjects, objects, and protection of civilians and civilian infrastructure. In addition, the author also looks for the urgency behind the formation of the rule of law, such as fulfilling the physical impact as a result of the attack and the Tallinn Manual guidelines in the form of soft law. This research was conducted using the Geneva Conventions and other rules governing armed conflict. Supported by other sources, such as UN documents and literature sources of books, journals, and articles. Based on the research results obtained, there is still an urgency for the state to establish international humanitarian law regarding cyber warfare.

Keywords: *Cyber Warfare, International Humanitarian Law, Computer Network Attack*

KATA PENGANTAR

Puji dan syukur Penulis panjatkan kepada Tuhan Yang Maha Esa atas berkat dan karunia yang telah dilimpahkan-Nya sehingga Penulis dapat menyelesaikan penulisan hukum yang berjudul "**Urgensi Pembentukan Instrumen Hukum Humaniter Internasional Tentang *Cyber Warfare***". Penulisan hukum ini merupakan salah satu syarat untuk menyelesaikan program Pendidikan Sarjana pada Fakultas Hukum Univesitas Katolik Parahyangan.

Penulis sadar bahwa penulisan hukum yang disusun ini masih memiliki banyak kekurangan karena berbagai tingkat kesulitan dalam penyusunan penulisan hukum ini. Namun berkat bimbingan, dorongan, semangat, dan bantuan dari berbagai pihak, akhirnya penulisan hukum ini dapat diselesaikan. Oleh karena itu, Penulis mengucapkan terima kasih kepada:

1. Tuhan Yang Maha Esa karena telah memberikan penguatan dan mendampingi penulis selama proses penyusunan penulisan hukum ini.
2. Papa, mama, dan adik penulis yang terkasih telah senantiasa memberikan semangat, dukungan, serta doa yang tak terputus kepada penulis selama proses penyusunan penulisan hukum ini.
3. Bapak Adrianus Adityo Vito Ramon, S.H., LL.M. (Adv.), selaku dosen pembimbing yang telah bersedia meluangkan waktu serta kesempatan selama proses penyusunan penulisan hukum ini.
4. Bapak Christian Donny Putranto, S.H., LL.M. dan segenap keluarga ICRC lainnya yang telah bersedia untuk mengadakan kuliah umum dan membantu menjawab pertanyaan-pertanyaan yang dilontarkan selama kuliah berlangsung.
5. Ibu Ursula N. Langouran, S.H. yang telah meluangkan waktu untuk berdiskusi lebih lanjut mengenai topik-topik yang masih harus didiskusikan yang kemudian termuat dalam penulisan hukum ini.
6. Shaunelee Alcinia Yanni, S.H. selaku sahabat baik penulis yang selalu mendukung, memberikan semangat, dan tak pernah berhenti untuk mendoakan penulis. Penulis

sangat berterimakasih karena telah menemani dari semester 1 hingga selesainya penulisan hukum ini.

7. Mellyanda Ratu selaku teman seperjuangan penulisan hukum penulis, terimakasih sudah mendengarkan keluh-kesah penulis. Sekaligus memberikan banyak masukan bagi penulis selama proses penyusunan penulisan hukum.
8. Vanessa Jesslyn Wijaya selaku sahabat lama yang menemani dari Sekolah Menengah ke Atas hingga penulis menyelesaikan pendidikan di UNPAR. Sekaligus, penulis turut berterimakasih sebesar-besarnya karena membantu untuk mendapatkan sumber materi ataupun bahan bacaan jurnal asing.
9. Oda Bintang Nagoya selaku sahabat penulis yang selalu menghibur dan menemani saat tengah menyusun penulisan hukum ini. Penulis juga sangat berterimakasih karena telah membantu menyelesaikan permasalahan pasca pengumpulan penulisan hukum.
10. Dahlah, Simbah, Hesa, Belman, dan Adrian selaku teman seperjuangan penulis yang selalu menghibur dan memberikan semangat di kala penulis sedang menghadapi kesulitan.

Bandung, 2 Juli 2024

Penulis,

Stephanie Liestia Gunawan

DAFTAR ISI

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perang atau yang dikenal dengan istilah "konflik bersenjata" merupakan sebuah fenomena kekerasan yang bersifat kolektif dan terorganisir yang mampu memengaruhi hubungan antara dua atau lebih sebuah negara yang diatur menggunakan sebuah hukum internasional yang diberi nama hukum humaniter internasional. Konsep hukum humaniter internasional untuk menjaga kontrol, disiplin, dan efisiensi dari para pasukan militer. Hal tersebut dijalankan dengan batasan dampak kekerasan dan penghancuran terhadap integritas fisik dan mental para kombatan.Konsep ini merupakan rangka dalam memfasilitasi kembalinya kombatan dalam masyarakat pasca berakhirnya konflik.[1] Perlahan, hukum humaniter mulai beradaptasi dengan perkembangan konflik bersenjata dimana banyak aktor non-negara yang turut andil menjadi bagian dari aktor utama kemunculan sebuah konflik bersenjata hingga adanya urgensi bagi warga negara untuk melindungi para warga sipil.[2]

Perkembangan dalam hukum humaniter internasional ini tertuang dalam *Geneva Conventions* (Konvensi Jenewa) Tahun 1949 beserta *Additional Protocol* (Protokol Tambahan) I dan II yang mengatur tentang prinsip-prinsip dalam hukum humaniter internasional serta konflik bersenjata baik internasional maupun non-internasional.[3] Menurut sejarah, penggunaan kekuatan militer yang dimaksud mengacu pada penggunaan pasukan bersenjata dan senjata konvensional seperti, tank, artileri, pesawat tempur, kapal tempur, dan infanteri dalam sebuah konflik bersenjata konvensional.[4] Penggunaan senjata konvensional telah menjadi aspek utama dalam sebuah konflik bersenjata, namun di era modern yang mana Teknologi

---

[1] ICRC," ICRC Position: How is The Term Armed Conflict Defined in Humanitarian Law", *ICRC*, 17 Maret,2008 , https://guide-humanitarian-law.org/content/article/3/war/, (diakses pada 15 Oktober 2023).
[2] *ibid.*
[3] *ibid.*
[4] Oona A. Hathaway dkk."What is a War Crime?", The Yale Journal of International Law 44.no.1 (2019): 62.

Komunikasi dan Informasi (TIK) ternyata menjadi salah satu hal yang memengaruhi perkembangan dari penggunaan kekuatan militer. Khususnya, penggunaan senjata siber (*cyber weapon*) yang menjadi salah satu tantangan kompleks. *Cyber weapon* menjadi salah satu isu yang menyita perhatian negara karena dapat memicu sebuah konflik bersenjata modern yang bisa disebut sebagai konflik bersenjata menggunakan metode siber (*cyber warfare*).[5]

Cyber warfare merupakan sebuah metode yang mengacu pada penggunaan sarana dan metode siber (*means and methods*) militer dalam situasi konflik bersenjata dalam suatu *cyberspace*. *Cyberspace* merupakan jaringan infrastruktur informasi dan komunikasi digital yang saling terhubung secara global. Hal ini meliputi internet, jaringan telekomunikasi, sistem komputer, dan informasi yang ada di dalamnya.[6] *Cyberspace* terdiri dari tiga lapisan; lapisan fisik yang meliputi energi listrik, sirkuit terpadu, infrastruktur komunikasi, serat optik, pemancar; Lapisan kedua sebagai lapisan perangkat lunak yang terdiri dari program komputer yang memproses informasi; dan lapisan ketiga sebagai lapisan yang paling tidak konkret, yaitu data.[7] Lapisan-lapisan yang terdapat dalam *cyberspace* ini dapat dikategorikan sebagai suatu infrastruktur kritis nasional dari suatu negara.[8]

Fakta bahwa *cyber warfare* dilakukan dalam *cyberspace* tidak mengecualikan bahwa *cyber warfare* dapat menghasilkan efek kinetik atau efek non-elektronik lainnya di luar *domain* siber dan bahkan mungkin secara khusus dimaksudkan oleh penyerang. Misalnya, target perang siber dapat mencakup individu yang kehidupannya atau fungsionalitas objeknya bergantung pada sistem komputer, seperti pembangkit listrik, sistem transportasi, atau orang-orang yang

---

[5] Michael N Schmitt dan Sean Watts, "The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare", Texas International Law Journal 50 (2015): 189 dan 222.

[6] Nils Melzer, "Cyberwarfare and International Law", UNIDIR RESOURCES (2011): 4.

[7] A Liaropoulos, "Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction?", Journal of Information Warfare (2012): 21.

[8] Beberapa contoh infrastruktur kritis nasional, seperti perbankan dan keuangan, minyak, gas dan listrik, air dan transportasi yang bergantung pada operasi jaringan komputer sehingga tidak bisa lepas dari kontrol negara. *ibid.*22.

terhubung dengan sistem pendukung kehidupan medis, militer atau profesional.[9] Salah satu contohnya, penyerangan yang dialami oleh Georgia di tahun 2008 menggunakan *cyber attack* dengan metode sistem *Distributed Denial of Service* (DDoS). Akan tetapi, para pakar hukum internasional belum bisa mendefinisikan *cyber weapon* itu sendiri dan belum memberikan tolak ukur bagi serangan siber (*cyber attack*) dengan tujuan untuk mencegah kemunculan *cyber warfare*.[10]

Sejauh ini doktrin militer hanya mendefinisikan arti dari senjata (*weapon*), yakni senjata yang secara eksplisit dirancang dan terutama digunakan untuk melumpuhkan personel atau materiil, sambil meminimalkan korban jiwa, cedera permanen pada personel, dan kerusakan yang tidak diinginkan pada properti dan lingkungan.[11] Secara spesifik, hukum yang mengatur tentang konflik bersenjata, khususnya Konvensi Jenewa Tahun 1949 belum mengatur mengenai penggunaan senjata siber sebagai bagian dari senjata yang dapat digunakan selama berkonflik.[12] Ditemukannya kekosongan hukum terkait *cyber weapon* juga berpengaruh terhadap fenomena *cyber attack* yang dialami oleh negara. *Cyber attack* merupakan sebuah aktivitas yang telah direncanakan untuk menghancurkan sebuah jaringan dan komputer atau untuk mencapai tujuan yang bersifat sosial, ideologis, agama, politik, atau tujuan sejenis, atau memiliki maksud untuk mengintimidasi pihak tertentu.[13]

Metode *cyber attack* kerap dikaitkan dengan pelaksanaan sebuah *cyber warfare*. Oleh karena itu, frasa "kerusakan terhadap fisik" tidak berlaku karena jika

---

[9] Nils Melzer.*loc.cit*.5.

[10] Stefano Mele, "Legal Considerations on Cyber Weapons and Their Definition", J.L&Cyberwarfare 3.no.1.(2014): 57.

[11] Department of Defence, "DOD Dictionary of Military and Associated Terms", Federation of American Scientist JP 1-02. (2013): 229-230.

[12] Pasal 36 Protokol I Konvensi Jenewa Tahun 1977 yang melarang penggunaan senjata seperti, penggunaan senjata beracun, penggunaan senjata biologis, penggunaan senjata kimia, penggunaan herbisida dalam kondisi tertentu, penggunaan efek senjata yang tujuannya adalah untuk melukai pecahan-pecahan yang tidak dapat terdeteksi sinar-x dan lain-lain.
J.-M. Henckaerts and L. Doswald-Beck (eds.), *Customary International Humanitarian Law*, (Cambridge: Cambridge University Press, 2005),251-292.

[13] Joseph N. Madubuike-Ekwe, "Cyber Attack and The Use of Force in International Law", Beijing Law Review 12. (2021): 633-634.

sebuah mesin atau infrastruktur tidak dapat lagi berfungsi secara normal karena serangan siber atau dampak dari gangguan siber, maka infrastruktur tersebut menjadi tidak efektif sebagaimana seharusnya sesuai dengan tujuannya.[14] Selain itu, masih belum terdapat definisi yang pasti dari '*cyber attack*' dalam hukum internasional dan negara masih mengalami kesulitan untuk mengidentifikasi subyek yang melakukan penyerangan sehingga sulit untuk dimintakan pertanggung jawaban. Mengingat pihak yang paling merasakan dampak dari kerusakan infrastruktur ini ialah para masyarakat sipil.[15]

Masyarakat sipil sangat bergantung pada keberlangsungan infrastruktur kritis sebuah negara, seperti perbankan dan keuangan, minyak, gas dan listrik, air dan transportasi yang bergantung pada operasi jaringan komputer.[16] Serangan *cyber attack* terhadap infrastruktur kritis akan menyebabkan, mengganggu fasilitas umum, menggagalkan proyek pemerintah, melemahkan perekonomian negara, merusak jaringan listrik, dan sebagainya.[17] Dampak dari *cyber attack* sendiri juga bisa mencapai skala global karena tipe penyerangan ini dapat diluncurkan untuk menargetkan negara, wilayah, bisnis, fasilitas kesehatan, dan organisasi militer mana pun.[18] Solusi untuk menangkis tipe penyerangan ini, ialah setiap negara harus sistem keamanan siber (*cyber security*).[19] Kehadiran *cyber security* diharapkan mampu memperkuat sistem keamanan siber nasional suatu negara. Oleh karena itu, dampak dari *cyber attack* juga menjadi bagian dari urgensi pembentukan instrumen hukum humaniter internasional tentang *cyberwarfare*.

Salah satu contohnya, pada tanggal 13 Agustus 2008, penyerangan yang dilakukan Rusia terhadap Georgia merupakan kasus penyerangan *cyber attack*.

---

[14] Zen Chang, "Cyberwarfare and International Humanitarian Law", Creighton International and Comparative Law Journal 9, no.1, (2017): 33-35.
[15] *ibid.*
[16] A Liaropoulos.*loc.cit*.22.
[17] R.A.Atrews "Cyberwarfare: Threats, Security, Attacks, and Impact", Journal of Information Warfare 19.no.4 (2020): 23.
[18] *ibid*.26.
[19] Susan W Berner dan Leo Clarke, "Civilians in Cyber Warfare Casualties", Singapore Management University Science and Technology Law Review 13, (2020): 251-252.

Penyerangan tersebut dapat dikategorikan sebagai penyerangan dengan sistem DDoS. Hal ini berkesesuaian dengan pengaturan dalam Pasal 49 Protokol Tambahan I Konvensi Jenewa Tahun 1977. Penyerangan tersebut memenuhi dua unsur pasal yakni menyebabkan kerusakan terhadap objek dan adanya penggunaan kekerasan selama penyerangan siber. Hal tersebut dibuktikan dengan adanya kelumpuhan beberapa situs pemerintahan seperti situs Kementerian Luar Negeri Georgia yang akhirnya terpaksa menjalankan operasionalnya dalam situs berbentuk "blogspot". Penyerangan yang dilakukan dengan sistem DDoS bersifat kinetik dapat menyebabkan korban jiwa jika aktivitas dan infrastruktur negaranya didasarkan dengan teknologi.

Saat ini, sekelompok ahli di bidang hukum internasional merancang sebuah panduan terkait penggunaan TIK dalam konteks konflik bersenjata.[20] Panduan tersebut bernama Manual Tallinn yang merupakan sebuah perjanjian internasional yang bersifat informal karena tidak sesuai memenuhi syarat dalam Pasal 38 ayat (1) Statuta Mahkamah Internasional tentang sumber hukum internasional. Hal ini juga didasari bahwa kerjasama internasional yang menghasilkan sumber hukum internasional praktiknya dilakukan di bawah organisasi internasional yang bersifat formal, seperti PBB. Pembentukan pedoman manual Tallinn tidak berada dibawah PBB, melainkan organisasi milik NATO bernama CCDCOE yang bekerja sama dengan para ahli di bidang teknologi. Sekelompok ahli tersebut tidak memiliki kuasa untuk mewakili negara manapun.[21] Oleh karena itu, Manual Tallinn dapat dikategorikan sebagai hukum internasional yang bersifat informal (*soft law*) sehingga dibutuhkan sebuah perjanjian internasional tentang *cyber warfare*.[22]

Urgensi pembentukan perjanjian internasional tentang *cyber warfare* juga meliputi prinsip kedaulatan negara dalam *cyberspace* untuk menjaga keamanan

[20] *ibid.*
[21] *ibid.*
[22] Phauline Charlotte Janssens dan Jan Wouters, "Informal International Law-Making: A Way Around The Deadlock of International Humanitarian Law?", *IRRC No.920-921*, November 2022, https://international-review.icrc.org/articles/informal-international-law-making-a-way-around-the-deadlock-of-ihl-920, (diakses pada 1 Maret 2024).

internasional.[23] Prinsip kedaulatan dalam *cyberspace* memberikan wewenang dan tanggung jawab atas penggunaan TIK.[24] Pertanggung jawaban yang diemban oleh negara tak hanya di dalam wilayahnya saja, tetapi juga diluar wilayah negara tersebut.[25] Pada hakikatnya, prinsip kedaulatan sendiri bukanlah aturan yang mengikat secara mandiri dengan mekanisme penegakan yang spesifik. Melainkan hanya memberikan kerangka dasar untuk pengembangan dan penafsiran aturan serta norma dalam hukum internasional.[26]

Sebagaimana yang telah dijabarkan dalam paragraf sebelumnya, terdapat urgensi pembentukan instrumen hukum internasional yang mengatur *cyber warfare*. Urgensi ini datang dari kondisi kekosongan hukum internasional yang hingga ini masih belum mengatur tentang *cyber warfare*. Tak hanya itu, terdapat beberapa alasan lain yang mendukung dari faktor urgensi ini, yakni; Potensi *cyber attack* yang dapat menimbulkan dampak luas yang menyebabkan kerusakan besar dan meluas, termasuk terhadap infrastruktur kritis, ekonomi, dan kehidupan sehari-hari; Perlindungan bagi warga sipil; Keterlibatan aktor non-negara; Koordinasi internasional antar negara dan tanggung jawab negara; dan Penguatan keamanan internasional.

Oleh karena itu, instrumen ini perlu mencakup aspek-aspek seperti: metode yang digunakan *cyber warfare*, perlindungan infrastruktur kritis (pembangkit energi, air dan limbah, jaringan telekomunikasi, keuangan, pertahanan dan keamanan, pangan pertanian, pertahanan dan keamanan, serta kebijakan informasi publik)[27], subjek dalam *cyber warfare*, objek militer dalam *cyber warfare* dan

[23] Lihat Dokumen UN.Doc.A/76/135.p.6.
[24] *ibid*.p.17.
[25] Garry P.Corn dan Robert Taylor, "Symposium of Sovereignity, Cyberspace, and Tallinn Manual 2.0 Sovereignity in The Age of Cyber",Cambridge University Press (2017): 209.
[26] *ibid.*
[27] Ketika menggunakan TIK dalam konteks konflik bersenjata, kewajiban untuk mengarahkan serangan siber hanya pada sasaran militer (obyek militer) menjadi suatu hal yang sangat penting. Menurut hukum humaniter internasional, sasaran militer harus dibatasi pada objek yang karena sifat, lokasi, tujuan, atau penggunaannya memberikan kontribusi efektif terhadap aksi militer dan yang kehancuran sebagian atau seluruhnya,atau netralisasi, dalam situasi yang berlaku pada saat itu, memberikan keuntungan militer yang pasti. Hal ini berarti bahwa infrastruktur sipil (termasuk pembangkit listrik dan air, properti pribadi, atau peralatan dan infrastruktur

pertanggungjawaban selama pelaksanaan *cyber warfare* khususnya dalam melindungi masyarakat sipil.[28] Dengan demikian, faktor urgensi yang telah dijabarkan menjadi salah satu alasan penguat bagi penulis untuk membuat sebuah penelitian berjudul, "**Urgensi Pembentukan Instrumen Hukum Humaniter Internasional Tentang *Cyber Warfare*".**

1.2 Rumusan Masalah

Bertolak dari latar belakang yang telah dipaparkan. Penulis merincikan beberapa pertanyaan yang menjadi topik pembahasan dalam kajian penelitian ini:

1. Bagaimana urgensi pembentukan instrumen hukum humaniter internasional mengenai *cyber warfare*?
2. Apa saja hal-hal yang perlu diatur dalam instrumen hukum humaniter internasional terkait *cyber warfare*?

1.3 Tujuan dan Penelitian

Sebagaimana yang telah dicantumkan dalam rumusan masalah di atas, berikut penulis paparkan maksud dan tujuan dari penelitian ini:

1. Menelusuri urgensi dibalik pembentukan instrumen hukum humaniter internasional yang secara khusus mengatur tentang *cyber warfare* dengan menggunakan tiga pertimbangan, yakni dampak fisik yang dihasilkan oleh *cyber attack*, penerapan kedaulatan dalam *cyber space*, dan Manual Tallinn yang hanya berbentuk panduan (*soft law*).
2. Memberikan gagasan mengenai substansi yang akan diatur, yakni metode yang digunakan untuk *cyber warfare*, perlindungan terhadap infrastruktur kritis serta masyarakat sipil, pihak yang terlibat dalam *cyber warfare*, dan metode yang

TIK pemerintah sipil) atau objek sipil lainnya tidak boleh diserang. Pernyataan ini merujuk pada artikel ICRC, "The Principle of Distinction in The Use of Information and Technology": 2-3.

[28] ICRC, " ICRC Position Paper: International Humanitarian Law and Cyber Operations during Armed Conflicts", Submitted to the 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' and the 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', (2019):3-5.

digunakan selama *cyber warfare* menurut kerangka hukum humaniter internasional.

Adapun manfaat yang dapat ditemukan selama melakukan penelitian yakni:

1. Manfaat Teoretis

   Melalui penelitian ini, manfaat yang penulis berikan ialah sumbangan ilmu pengetahuan dalam bidang hukum humaniter internasional terkait penyusunan instrumen hukum internasional mengenai *cyber warfare* dapat mengisi kekosongan hukum yang saat ini ada dalam pengaturan konflik bersenjata di dunia maya. Melalui penelitian ini, akan tercipta landasan hukum yang jelas untuk menangani serangan cyber dalam konteks humaniter internasional, menciptakan norma-norma yang dapat diakui secara universal.

2. Manfaat Praktis

   Melalui penelitian ini, manfaat yang penulis berikan ialah menggagas adanya pembentukan instrumen hukum humaniter internasional terkait pengaturan *cyber warfare* yang memiliki kekuatan hukum mengikat dan sifat memaksa bagi negara-negara yang menjadi negara pihak dari perjanjian internasional tersebut. Sekaligus, pembentukan instrumen hukum humaniter internasional ini membantu para praktisi untuk dapat mengaplikasikannya ke dalam kasus *cyber warfare* di masa depan.

1.4 Metode Penelitian

Metode penelitian yang digunakan dalam penulisan hukum ini adalah metode yuridis normatif. Penelitian hukum yuridis normatif merupakan pendekatan penelitian yang berfokus pada analisis hukum dan peraturan yang ada dengan tujuan memahami, mengevaluasi, dan menginterpretasi norma hukum serta teori hukum yang mendasarinya. Penulis menggunakan penelitian yuridis normatif bertajuk "Urgensi Pembentukan Instrumen Hukum Humaniter Internasional Terkait Pengaturan *Cyber Warfare*" yang berfokus adanya urgensi bagi hukum humaniter internasional untuk membentuk sebuah aturan mengenai *cyber warfare* yang dinilai menjadi ancaman terhadap keamanan global. Penulis akan menyajikan secara

deskriptif mengenai pokok-pokok pembahasan yang sudah dimunculkan dalam rumusan masalah menggunakan konsep dan teori yang sudah tersedia beserta data yang mendukung penulisan ini.[29]

1.5 Teknik Pengumpulan Data

Teknik pengumpulan data yang dilakukan oleh penulis didasarkan pada studi kepustakaan yang dilakukan dengan pengumpulan data terhadap buku-buku di pusat pustaka serta melalui penelusuran di internet. Semua data yang diperoleh dalam penelitian ini akan mengalami analisis sistematis dengan penerapan metode kualitatif. Hasil dari analisis data tersebut akan diungkapkan dalam bentuk deskripsi dengan maksud untuk menjawab tujuan dan masalah yang diajukan dalam penelitian ini. Secara spesifik, sumber-sumber tersebut dibagi menjadi sumber hukum primer dan sumber hukum sekunder yang akan dijabarkan sebagai berikut:

1. Sumber Hukum Primer

   Sumber hukum primer yang akan digunakan oleh penulis dalam menyusun penelitian ini ialah Piagam Perserikatan Bangsa-Bangsa, Konvensi Den Haag Tahun 1809 dan Tahun 1907, Konvensi Jenewa Tahun 1949 serta Protokol Tambahan I dan II Tahun 1977, dan Aturan Hukum Kebiasaan Humaniter Internasional.

2. Sumber Hukum Sekunder

   Sumber hukum sekunder yang digunakan oleh penulis dalam menyusun penelitian diperoleh mendukung sumber hukum primer melalui United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN.Doc A/76/135), Manual Tallinn (1.0 dan 2.0) yang didukung dengan buku, jurnal, dan artikel sebagai karya yang diluncurkan oleh para akademisi.

[29] Soejono Soekanto. *Pengantar Penelitian Hukum Normatif*.Cetakan ke 14 (Depok: UI Press,2014): 203-205.

1.6 Sistematika Penulisan

Sistematika penulisan akan terstruktur dalam beberapa tahap yang akan dikenal sebagai bab-bab. Setiap bab akan menjelaskan permasalahan yang terkait satu sama lain dalam konteks yang terintegrasi. Penulisan akan terdiri dari lima bab yang akan dirancang sebagai berikut:

BAB I PENDAHULUAN

Bab ini akan berisi informasi umum tentang tahapan penelitian, termasuk konteks latar belakang penelitian, perumusan masalah, tujuan dan kepentingan penelitian, pendekatan metodologi yang digunakan dalam penelitian, dan tata cara penyusunan tulisan ini.

BAB II TINJAUAN UMUM CYBER WARFARE DALAM HUKUM HUMANITER INTERNASIONAL

Bab ini menyajikan kerangka teoritis yang mendasari penelitian ini. Kerangka teoritis ini diawali dari konsep dasar hukum humaniter internasional serta perkembangannya yang dipengaruhi oleh perkembangan teknologi. Selama ini, instrumen hukum humaniter internasional belum memberikan batasan yang jelas mengenai pelaksanaan *cyber warfare*. Oleh karena itu, masih terdapat kekosongan hukum yang belum sepenuhnya mengatasi tantangan yang muncul dalam *cyber warfare*. Hal ini menyebabkan adanya urgensi untuk membentuk sebuah instrumen hukum humaniter internasional tentang *cyber warfare.*

BAB III *CYBER WARFARE* DALAM KONTEKS KONFLIK BERSENJATA MODERN

Bab ini akan membahas mengenai elemen dalam *cyber warfare* dalam konteks konflik bersenjata modern. Elemen-elemen yang dimaksud diantaranya, cyber attack sebagai metode penyerangan,

cyber weapon sebagai alat (malware) yang digunakan untuk menyerang, obyek dari *cyber warfare*, dan peran *cyber security* dalam mencegah *cyber attack*. Terutama, penulis ingin menekankan dampak dari *cyber warfare* yang memiliki kemungkinan untuk menimbulkan dampak fisik. Sebagai contoh, penulis akan membahas kasus cyber attack yang dialami oleh Pemerintah Georgia di tahun 2008 yang bersamaan dengan kasus invasi Rusia terhadap Georgia.

BAB IV URGENSI PENGATURAN CYBER WARFARE DALAM HUKUM HUMANITER INTERNASIONAL

Bab ini menjabarkan mengenai urgensi dari pembentukan sebuah instrumen hukum humaniter internasional. Urgensi ini mencakup aplikasi prinsip kedaulatan dalam *cyber space* dan dampak dari serangan *cyber attack*. Prinsip kedaulatan diaplikasikan dalam konteks negara memiliki hak dan tanggung jawab untuk melindungi wilayahnya, termasuk ruang siber. Aplikasi dari prinsip kedaulatan ini dapat membantu negara memitigasi dampak dari *cyber attack*. Hal ini dikarenakan, *cyber attack* dapat mengganggu dan merusak infrastruktur kritis, mengancam keamanan nasional maupun internasional, dan warga sipil. Oleh karena itu, dibutuhkan sebuah aturan mengenai elemen-elemen yang harus diatur dalam hukum humaniter internasional tentang *cyber warfare*. Beberapa diantaranya, yaknimetode yang digunakan *cyber warfare*, perlindungan infrastruktur kritis, subjek yang boleh diserang, dan objek militer.

BAB V KESIMPULAN

Pada bab terakhir, penulis akan merangkum temuan dari penelitian hukum ini dan juga mengusulkan rekomendasi yang

dianggap memiliki nilai kontribusi terhadap perkembangan hukum humaniter internasional.