BAB V

KESIMPULAN

5.1 Kesimpulan

Cyber warfare merupakan sebuah jenis konflik bersenjata terbaru sehingga dibutuhkan batasan-batasan untuk mencegah dampak berlebihan kepada masyarakat sipil. Pada dasarnya, batasan-batasan tersebut merupakan prinsip-prinsip HHI yang bertujuan untuk melindungi baik pihak yang terlibat maupun tidak terlibat dalam konflik bersenjata. Adanya gagasan mengenai urgensi untuk membentuk instrumen HHI yang mengatur secara khusus tentang *cyber warfare*. Tujuan dibalik pengaturan ini, ialah untuk memaksa negara-negara untuk tunduk dan mengikuti aturan HHI tersebut apabila hendak melakukan *cyber warfare*. Akan tetapi, usulan mengenai pembentukan hukum internasional tentang *cyber warfare* sendiri masih membutuhkan pertimbangan dari seluruh negara.

Pertimbangan pembentukan hukum internasional dari negara mencakup kondisi politik, ekonomi, dan kepentingan nasional suatu negara. Kondisi-kondisi tersebut menyebabkan negara enggan (*reluctant*) untuk mengikatkan diri kepada suatu perjanjian internasional. Selain itu, pembentukan perjanjian internasional sendiri dapat memakan waktu yang lama karena proses persetujuan mulai dari penandatanganan, pertukaran instrumen, ratifikasi, penerimaan, persetujuan, ataupun aksesi. Terlebih, membutuhkan waktu yang lama bagi negara untuk menyepakati aspek-aspek yang harus diatur dalam perjanjian internasional tersebut. Dengan demikian, adanya usulan *model law* sebagai pedoman penyusunan hukum domestik ataupun perjanjian internasional.

Pertimbangan untuk menyusun sebuah *model law* tentang *cyber warfare* dilatarbelakangi oleh harmonisasi internasional sehingga menciptakan kerangka hukum yang dapat membantu negara-negara dalam mengembangkan hukum yang konsisten dan seragam. Selanjutnya, *model law* membantu merumuskan hukum

domestik yang efektif dan sesuai dengan standar internasional, mengurangi ambiguitas hukum, dan meningkatkan efektivitas penegakan hukum. Terakhir, *model law* memiliki sifat fleksibel dan dapat disesuaikan dengan konteks spesifik negara masing-masing. Hal ini memungkinkan negara untuk mengadopsi elemen-elemen yang relevan sesuai dengan kebutuhan dan prioritas nasional mereka dalam menghadapi ancaman *cyber warfare*.

Model law dapat digunakan untuk membentuk baik hukum internasional maupun sebuah hukum domestik. *Model law* sebagai pedoman bagi hukum domestik memberikan akses untuk negara-negara dapat menciptakan regulasi domestik yang efektif dalam menangani isu-isu terkait *cyber warfare*. Negara dapat memastikan bahwa hukum domestik mereka konsisten dengan standar internasional. Sementara, *model law* dapat mempermudah negara-negara dalam merumuskan dan mengimplementasikan perjanjian internasional terkait *cyber warfare*. Dengan dasar hukum yang seragam, negara-negara dapat lebih mudah menyepakati kerangka kerja dan protokol internasional untuk penanggulangan dan pencegahan *cyber attack*.

Oleh karena itu, jika negara-negara ingin membuat sebuah hukum internasional ataupun *model law*. Berikut beberapa hal yang harus dimuat dalam *model law* tersebut, yakni:

1. *Cyber attack* dapat diklasifikasikan sebagai sebuah serangan dengan dasar hukum Pasal 49 Protokol Tambahan I Konvensi Jenewa Tahun 1977, terutama jika operasi tersebut bersifat ofensif dan menghasilkan dampak langsung kepada warga sipil atau infrastruktur kritis. Akan tetapi, masih terdapat perdebatan mengenai penerapan hukum humaniter internasional dalam operasi siber, terlebih dalam konteks obyek '*dual-use*' yang dapat digunakan baik untuk kepentingan sipil maupun militer. Oleh karena itu, dibutuhkan penelitian lebih lanjut mengenai penerapan prinsip-prinsip hukum humaniter internasional, seperti prinsip kemanusiaan, kebutuhan

militer, proporsionalitas, dan pembeda untuk mencegah dampak akibat *cyber attack*.

2. *Cyber weapon* bisa dianggap sebagai "senjata" dalam Pasal 36 API Konvensi Jenewa Tahun 1977 dan *Martens Clause* meskipun belum tentu menghasilkan efek fisik secara langsung, seperti senjata konvensional pada umumnya. Akan tetapi, penulis menggunakan pertimbangan bahwa *cyber weapon* dapat digunakan untuk menyerang, merusak, atau menganggu sistem atau jaringan komputer. Oleh karena itu, emiliki potensi untuk menyebabkan kerusakan atau bahaya. Misalnya, serangan siber dapat merusak infrastruktur kritis, menyebabkan gangguan terhadap keamanan negara, atau membocorkan informasi rahasia.
3. Obyek '*dual-use*' yang digunakan untuk tujuan sipil dan militer dapat diklasifikasikan sebagai objek militer dalam konteks tertentu. Menurut Pasal 52 ayat (2) Protokol Tambahan I Konvensi Jenewa Tahun 1977, suatu obyek dapat dianggap sebagai objek militer berdasarkan empat kriteria: sifat, lokasi, tujuan, atau penggunaan. Selain itu, objek tersebut harus berkontribusi aktif terhadap aksi militer dan penghancuran, penangkapan, atau netralisasinya harus memberikan keuntungan militer yang jelas. Dalam konteks siber, obyek seperti jaringan komputer sipil dapat menjadi target militer yang sah jika digunakan untuk mendukung aksi militer. Misalnya, jika jaringan komputer sipil digunakan untuk melancarkan serangan jaringan komputer atau jika digunakan oleh pasukan musuh untuk komunikasi militer, maka jaringan tersebut dapat dianggap sebagai target militer yang sah. Hal ini juga berlaku untuk negara-negara seperti Amerika Serikat, di mana banyak komunikasi militer disalurkan melalui jaringan sipil.

5.2 Saran

Berdasarkan kesimpulan yang telah dipaparkan dalam paragraf di atas, saran yang dapat diberikan oleh penulis mengenai persoalan urgensi dibalik kebutuhan untuk membentuk sebuah instrumen hukum humaniter internasional tentang *cyber warfare,* ialah

1. Kebutuhan untuk mengklasifikasi yang jelas kapan obyek '*dual-use*' dapat dikategorikan sebagai obyek militer dan kapan dikategorikan sebagai sebuah obyek sipil. Hal ini menyesuaikan dengan pertimbangan penggunaan infrastruktur siber apabila infrastruktur siber tersebut sekiranya dinilai memberikan keuntungan bagi operasi militer, maka dapat dianggap sebagai obyek militer yang sah. Sementara, jika infrastruktur siber tersebut digunakan untuk warga sipil, maka dibutuhkan pertimbangan lebih lanjut mengenai batasan dari penyerangan tersebut agar tidak menghasilkan dampak yang berlebihan.
2. Kebutuhan untuk melakukan peninjauan *cyber weapon* sebagai senjata, seperti yang diatur dalam Pasal 36 Protokol Tambahan I Konvensi Jenewa Tahun 1977. Penggunaan senjata siber seperti malware dan botnet dalam operasi militer menunjukkan bahwa metode dan sarana perang terus berkembang dan menimbulkan tantangan baru dalam penegakan hukum humaniter. Oleh karena itu, penting bagi negara-negara untuk terus mengembangkan prosedur internal yang efektif dalam meninjau dan mengatur penggunaan senjata siber, serta memastikan bahwa semua operasi militer mematuhi prinsip-prinsip hukum humaniter internasional.
3. Kebutuhan untuk melakukan penelitian lebih lanjut mengenai *cyber attack* sebagai sebuah serangan dalam konteks *cyber warfare*. Akan tetapi, penerapan definisi "serangan" dalam konteks ini masih menjadi perdebatan. Pendekatan yang terlalu luas dapat membuat gangguan kecil dianggap sebagai serangan. Beberapa pendapat menyarankan bahwa fokus seharusnya pada "permusuhan", yaitu operasi siber yang dirancang untuk merugikan musuh dan mempengaruhi operasi militer atau kapasitas militer. Oleh karena itu, penting untuk mempertimbangkan prinsip-prinsip hukum humaniter internasional seperti kemanusiaan, kebutuhan militer, proporsionalitas, dan pembeda dalam setiap operasi siber.

DAFTAR PUSTAKA

Buku:

Duncan Hodges and Sadie Creese, "Understanding Cyber-Attacks" dalam *Cyber Warfare a Multidiciplinary Analysis*, ed. James A. Green, New York: The Routledge Studies in Conflict, Technology and Security, 2015.

Frits Kalshoven dan Leisbeth Zegveld. *Constraint on The Waging of War 4th Edition*.United Kingdom: Cambridge University Press, 2011

Heather A. Harrison Dinnis. *Cyber Warfare and The Laws of War*.New York: Cambridge University Press, 2012.

Heather A. Harrison Dinnis. *The Regulation of Cyber Warfare Under Jus In Bello*.New York: Routledge Studies in Conflict, Security, and Technology, 2015.

J.M. Henckaerts and L. Doswald-Beck.*Customary International Humanitarian Law*. Cambridge: Cambridge University Press, 2005.

Neil.C.Rowe.*The Attribution of Cyber Warfare*.New York: Routledge Studies in Conflict, Security, and Technology, 2015.

Richard Stienon.*A Short History of Cyber Warfare*. New York: Routledge Studies in Conflict, Security, and Technology, 2015.

Robert Klop. *Advanced Introduction to International Humanitarian Law*. United States of America: Edward Edgar Alan Publishing Limited, 2014.

Soejono Soekanto. *Pengantar Penelitian Hukum Normatif*. Cetakan ke 14. Depok: UI Press, 2014.

Jeffrey Carr, *Inside Cyber Warfare*, California: O'Reilly Media, 2011.

Jurnal:

Amanda Alexander, "A Short History of International Humanitarian Law", The European Journal of Law 26.no.1 (2015): 115.

Anonim, "Cyber Attacks in Context of International Humanitarian Law", *UIO: Det Juridiske Fakultet* (2013):110.

Bart Hogeveen, “The UN Cyber Norms: How Do They Guide Responsible Development and Use of Offensive Cyber Capabilities”, The Cyber Defence Review 7.No.4 (2022):127.

Col. Matthew M. Hurley, “For and From Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance”, Air and Space Power Journal (2012):16.

Dan Efrony and Yuval Shany, “A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice”, American Journal of International Law112, no. 4. (2018):587.

Department of Defence, “DOD Dictionary of Millitary and Associated Terms”, US Military Defence Federation of American Scientist JP 1-02. (2013): 229-230.

Dieter Fleck, “Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual”, Journal of Conflict and Security Law 18, no. 2 (2013): 335–336.

Elizabeth Mavropoulou, “Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks”, Journal of Law and Cyber Warfare 4.no.2 (2015): 25-26.

Harriet Moynihan, “The Application of International Law to State Cyberattacks Sovereignty and Non-intervention”, The Royal Institute of International Affairs, (December 2019):12.para.31.

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

Lin H, “Cyber Conflict and International Humanitarian Law”, International Review of the Red Cross 94.no.886 (2012): 517.

Maj Gen P K Mallick, “Cyber Weapons-A Weapon of War?”, Vivekananda International Foundation, (2021): 6.

Michael N. Schmitt, “Classification of Cyber Conflict”, International Law Studies 89.(2013):239.

Michael N. Schmitt, “Cyber Operations and The Jus In Bello: Key Issues”, International Law Studies 87 (2015): 92-93.

Michael N. Schmitt, “The Law of Cyber Warfare: *Quo Vadis*?”, Stanford Law & Policy Review 25 (2013): 293.

Michael N.Schmitt, “Wired Warfare: Computer Network Attack and Jus In Bello”, IRRC June 84. No.846.(2002): 379.

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, Oxford Academic Press.

Myrna Azzopardi, “ The Tallinn Mannual on International Law Applicable to Cyber Warfare: a Brief Introduction on It’s Treatment of *Jus Ad Bellum* Norms”, Elsa Matla Law Review (ed.) III, (2013): 174.

Nils Melzer, “Cyberwarfare and International Law”, UNIDIR RESOURCES (2011): 4.

Oona A. Hathaway dkk.”What is a War Crime?”, The Yale Journal of International Law 44.no.1 (2019): 62.

Papanastasiou Afroditi, “Application of International Law in Cyber Warfare Operations”, Research Paper Published at SSRN, (2010):7.

Piret Pernik, “The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine”, European Union Institute for Security Studies. (2018):59.

R Fanelli, “Cyber Space Offense and Defence”, Journal of Information Warfare 15. No.2 (2016): 54.

Robert Kolb, *Advanced Introduction to International Humanitarian Law*, (United States of America: Edward Edgar Alan Publishing Limited, 2014).22-26.

Robin Gei,”The Conduct of Hostilities in and via Cyberspace”, American Society of International Law 104 (2010): 372-373.

Roxana Georgiana Radu, “The Monopoly of Violence in the Cyber Space: Challenges of Cyber Security” in Enrico Fels, Jan-Frederik Kremer and Katharina Kronenburg (eds.) Power in the 21st Century: International Security and International Political Economy in a Changing World” (Springer-Verlag Berlin Heidelberg, Germany, 2012): 144.

Sangeetha Prabhu dan Subramanya Bhat, “Cyber Attacks Mitigation: Detecting Malicious Activities in Network Traffic-A Review Literature”, International Journal of Case Studies in Business, IT, and Education 4. no.2,(2020): 45.

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

Susan W Berner dan Leo Clarke, “Civillians in Cyber Warfare Casualities”, Singapore Management University Science and Technology Law Review 13, (2020): 251-252.

U. M. Mbanaso, PhD and E.S. Dandaura, PhD, “The Cyberspace: Redefining a New World”, IOSR Journal of Computer Engineering 17. no.13 (2015): 17-18.

Zachary R.Orr, “Addressing Unlawful Cyber Operations in Armed Conflict Through Human Rights Bodies Instead of the International Criminal Court”, Vanderblit Journal of Transnasional Law 359 (2024): 365.

Zen Chang, “Cyberwarfare and International Humanitarian Law”, Creighton International and Comparative Law Journal 9, no.1, (2017): 33-35.

Artikel:

Cordula Droege and Eirini Giorgou, “How International Humanitarian Law Develops”, 2022, International Review of The Red Cross 104:1807.

International Red Cross Committee (ICRC),“The Law of War Imposes Limits On Cyber Attacks Too”,International Committee of the Red Cross, Juli 2013, https://www.icrc.org/en/doc/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm, (diakses pada 23 Oktober 2023).

IRRC, “International humanitarian law and cyber operations during armed conflicts ICRC position paper 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, November 2019”, International Review of The Red Cross Regarding Digital Technologies and War 102.no.913 (2020):486-489.

Konferensi

David Wallace, Jakub Harašta, dan Ivana Kudláčková, “Cyber Weapons Review in Situations Below The Threshold of Armed Conflict” dipresentasikan dalam 2020 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade (Estonia, 2020).99-102.

Roxana Georgiana Radu,“The Monopoly of Violence in the Cyber Space: Challenges of Cyber Security”,Enrico Fels, Jan-Frederik Kremer and Katharina

Kronenburg (eds.) dipresentasikan dalam Power in the 21st Century: International Security and International Political Economy in a Changing World (Springer-Verlag Berlin Heidelberg, Germany, 2012).144.

Internet:

Alexander S. Gillis, "Definition Cyber Warfare", *Techtarget*, Maret 2023, https://www.techtarget.com/searchsecurity/definition/cyberwarfare, diakses pada 29 April t2024.

Anonim, "Cyber Attack", *Imperva*, https://www.imperva.com/learn/application-security/cyber-attack/, diakses pada 29 April 2024.

Anonim, "The Cyber Raiders Hitting Estonia",*BBC News*, 18 Januari tahun 2011, http://news.bbc.co.uk/2/hi/europe/6665195.stm, (diakses pada 22 Desember tahun 2023).

Anonim, "What is a Cyber Attack", *CISCO*, 2017, https://www.imperva.com/learn/application-security/cyber-warfare/, diakses pada 29 April 2024.

Anonim, "What is a Cyber War-Explained", *New England Technology*, 30 Maret 2023, https://www.neit.edu/blog/what-is-a-cyber-war-explained#Types_of_Cyber_Warfare_Attacks, diakses pada 29 April 2024.

Anonim. "Venezuela Goes Dark in Massive Power Outwage", *DW*, Juli 2019, https://www.dw.com/en/venezuela-power-outage-causes widespread-chaos/a-47821661.

Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia", *The Guardian*, 17 Mei Tahun 2007, https://www.theguardian.com/world/2007/may/17/topstories3.russia, (diakses pada 20 Desember tahun 2023).

ICRC, "Geneva Conventions of 1949, Additional Protocols and Their Commentaries-Art. 2(1)", IHL Database, 2016, https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/introduction/commentary/2016?activeTab=1949GCs-APs-and-commentaries, (diakses pada 28 Oktober 2023).

ICRC, "What Limits Does The Law or War Impose On Cyber Attacks?",*International Committee of the Red Cross*, Juli 2013, https://www.icrc.org/en/doc/resources/documents/faq/130628-cyber warfare-q-and-a-eng.htm.

ICRC Database, Treaties, States Parties and Commentaries, Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949., Article 12 - Protection and care of the wounded and sick, https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-12, diakses pada tanggal 25 Maret tahun 2024.

ICRC Database, Treaties, States Parties and Commentaries, Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949., Commentary of 01.01.2016 , Introduction , https://ihl-databases.icrc.org/en/ihltreaties/gci1949/introduction/commentary/2016?activeTab=1949GCs-APs-and commentaries.

ICRC Database, Treaties, States Parties and Commentaries, Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea. Geneva, 12 August 1949., Article 13 - Protected persons, https://ihl-databases.icrc.org/en/ihl-treaties/gcii-1949/article-13, diakses pada tanggal 25 Maret tahun 2024.

ICRC Database, Treaties, States Parties and Commentaries, Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949., Commentary of 01.01.2020 , Article 3 - Conflicts not of an international character , https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-3/commentary/2020, diakses pada tanggal 20 Maret tahun 2024.

ICRC Database, Treaties, States Parties and Commentaries, Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949., Commentary of 01.01.2020 , Article 3 - Conflicts not of an international character , https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-3/commentary/2020, diakses pada tanggal 20 Maret tahun 2024.

ICRC Database, Treaties, States Parties and Commentaries, Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949., Commentary of 01.01.2020 , Article 3 - Conflicts not of an international character , https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-3/commentary/2020, diakses pada tanggal 25 Maret tahun 2024.

ICRC Database, Treaties, States Parties and Commentaries, Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949., Article 27 - Treatment I. General observations, https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/article-27, diakses pada tanggal 25 Maret tahun 2024.

ICRC Database, Treaties, States Parties and Commentaries, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of

Victims of International Armed Conflicts (Protocol I), 8 June 1977., Article 49 - Definition of attacks and scope of application, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-49 (Diakses pada 23 December of 2023).

International Red Cross Committee (ICRC),"The Law of War Imposes Limits On Cyber Attacks Too",*International Committee of the Red Cross*, Juli 2013, https://www.icrc.org/en/doc/resources/documents/interview/2013/06- 27-cyber-warfare-ihl.htm.

Jenna McLaughlin, "Inside Russia's Attempts to Hack Ukrainian Military Operation", *NPR*, Oktober 2023, https://www.npr.org/2023/08/10/1193167328/russia-hack-ukraine military.

Joshua Davis, "Hackers Take Down The Most Wired Country in Europe",*Wired*, 21 Agustus,Tahun 2007, https://www.wired.com/2007/08/ff-estonia/, (diakses pada 24 Desember tahun 2023).

Mark Lander dan John Markoff, "Digital Fears Emerge After Data Siege in Estonia", *New* York, 27 Juli Tahun 2007, https://www.nytimes.com/2007/05/29/technology/29estonia.html, (diakses pada 24 Desember tahun 2023).

Michael J. Addams, "A Warning About Tallinn Mannual 2.0..Whatever it Says", LAWFARE, 4 Januari 2017,https://www.lawfaremedia.org/article/warning-about-tallinn-20-%E2%80%A6-whatever-it-says, (diakses pada 7 April tahun 2024).

Miranda Sieg, "Denial-of-Service: The Estonian Cyberwar and It's Implications For U.S. National Security", *The International Affairs* Review,4 April, https://www.iar-gwu.org/blog/2009/04/04/denial-of-service-the-estonian-cyberwar-and-its-implications-for-u-s-national-security, (diakses pada 28 Desember 2023).

Oliver Buxton, "What is a Cyber Warfare", *Avast Academy*, 14 Juli tahun 2023, https://www.avast.com/c-cyber-warfare, diakses pada 29 April tahun 2024.

Dokumen Kasus:

Certain Activities carried out by Nicaragua in the Border Area (Costa Rica v Nicaragua), Judgment, ICJ Reports 2015, para. 93. Lihat juga Corfu Channel (Merits) Judgment 9 April 1949.

Lihat International Court of Justice in Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, 27 June 1986).

Prosecutor v. Limaj, Case No. IT-03-66-T, Judgment, ¶ 89 (Int'l Crim. Trib. for the former Yugoslavia 30 November 2005).

Prosecutor v. Tadić; Case No. IT-94-1-l, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction 13 August,1997).

Dokumen PBB:

UN GGE Reports A/70/237

Dokumen Publikasi Pemerintah Asing:

India Parliament Government Document No.35/RN/Ref./July/2017.