TATOHI
JURNAL ILMU HUKUM
Volume 2 Nomor 9, November 2022: h. 905 – 915 E-ISSN: 2775 - 619X

Tinjauan Yuridis Pelanggaran *Cyber Attack* Dalam Perang Modern Berdasarkan Hukum Humaniter Internasional

Stenly Pattiruhu[1], Johanis Steny Franco Peilouw[2], Wilshen Leatemia[3]

[1,2,3] Fakultas Hukum Universitas Pattimura, Ambon, Indonesia.
: pattiruhustenly@gmail.com
: 10.47268/tatohi.v2i9.1430

Info Artikel

Keywords:
Cyber Attack; Responbility; International Humanitarian Law.

Kata Kunci:
Cyber Attack; Tanggungjawab Negara; Hukum Humaniter Internasional.

Abstract

Introduction: *Violations in the form of cyber attacks are carried out by countries that have strong cyber space infrastructure against other countries that have weaknesses in their cyber defense systems.*
Purposes of the Research: *The purpose of this paper is to find out and understand the position of cyber attacks in international humanitarian law and to know and understand the state's responsibility for the use of cyber attacks.*
Methods of the Research: *This type of research is normative juridical where the research is carried out by collecting primary, secondary and tertiary data obtained using library research. The data that has been collected is analyzed qualitatively, the description of which is arranged systematically based on legal disciplines to achieve clarity on the issues to be discussed.*
Results of the Research: *The results of this study indicate that the position of cyber attacks in international humanitarian law is the same as conventional wars based on a cyber attack approach as a war domain as well as attacks in cyber attacks. Cyber attacks also violate the principles of humanitarian law, namely the Principle of Discrimination, the Principle of Proportionality and Uncessary Suffering. Furthermore, with regard to the state having an obligation to be responsible for violations of the principles of International Humanitarian Law caused by cyber attacks carried out by a person or group, it is proven to have a close relationship with the state in accordance with international customs regarding state responsibilities and is also obliged in the responsibilities contained in the law. United Nations Charter. Forms of liability can be in the form of cessation of attacks and reparations. The reparations themselves can be carried out by means of restitution, compensation and giving satisfaction to the victim country.*

Abstrak

Latar Belakang: Pelanggaran berupa cyber attack yang dilakukan oleh negara yang memiliki infrastruktur cyber space yang kuat terhadap negara lain yang memiliki kelemahan adalam sistem pertahanan sibernya.
Tujuan Penelitian: Penulisan bertujuan untuk mengetahui dan memahami kedudukan cyber attack dalam hukum humaniter internasional serta ntuk mengetahui dan memahami tanggung jawab negara terhadap penggunaan cyber attack.
Metode Penelitian: Tipe penelitian ini adalah yuridis normatif dimana penelitian dilakukan dengan cara mengumpulkan data primer, sekunder dan tersier yang diperoleh menggunakan studi kepustakaan. Data yang telah terkumpul dianalisis secara kualitatif yang penguraiannya disusun

secara sistematik berdasarkan disiplin ilmu hukum untuk mencapai kejelasan masalah yang akan dibahas.
Hasil Penelitian: Hasil dari penelitian ini menunjukan bahwa kedudukan cyber attack dalam hukum humaniter internasional sama seperti perang konvensional berdasarkan pendekatan cyber attack sebagai domain perang serta serangan dalam cyber attack. Cyber attack juga melanggar prinsip hukum humaniter yaitu Prinsip Pembedaan, Prinsip Proporsionalitas dan Uncessary Suffering. Selanjutnya,berkaitan dengan negara memiliki kewajiban bertanggungjawab atas pelanggaran prinsip Hukum Humaniter Internasional yang disebabkan oleh tindakan cyber attack yang dilakukan oleh seseorang maupun kelompok, terbukti memiliki keterkaitan erat dengan negara yang sesuai dengan kebiasaan internasional mengenai tanggungjawab negara dan juga berkewajiban dalam tanggung jawab yang terdapat dalam Piagam PBB. Bentuk pertanggungjawaban dapat berupa penghentian serangan dan reparasi. Reparasi sendiri dapat dilakukan dengan cara restitusi, kompensasi serta memberikan kepuasan kepada negara korban.

1. Pendahuluan

Kehidupan umat manusia pada era industri dan teknologi 4.0 cukup bergantung pada sesuatu yang disebut dengan *cyber space* atau biasa dikenal dengan dunia maya. Aktivitas *cyber space* dapat diakses oleh siapa saja yang ingin untuk mengolah data maupun informasi melalui sarana elektro dan elektro magnetik. Aktivitas ini bukan hanya dilakukan oleh tiap individu saja melainkan organisasi bahkan juga oleh pemerintahan suatu negara tertentu. Penguasaan negara terhadap penggunaan teknologi digital dan infrastrukturnya di dalam *cyber space* semakin berkembang. Dampak negatif yang timbul adalah ketika suatu negara mencoba menerobos infrastruktur sistem pertahanan *cyber space* atau biasa dikenal dengan istilah *cyber defence* dari negara yang laju perkembangannya cukup jauh dibawah negara tersebut. "Aktivitas *cyber attack* sendiri adalah untuk masuk pada jaringan sistem komputer suatu infrastruktur atau masuk pada server web dalam bentuk virus, worm dan trojan."[1]

Pada Larangan terhadap penggunaan banyak senjata, yang mencakup peluru bekas, senjata kimia dan biologi, senjata laser yang menyilaukan dan ranjau anti-personil diatur dalam hukum humaniter internasional. Secara umum dapat dilihat dalam Pasal 36 Protokol Tambahan I Konvensi Jenewa tahun 1977 yakni:[2] *In the study, development, acquisition, or adoption of a new weapon, means or method of warfare, a high contracting party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this protocol or by any other rule of international law applicable to the high contracting party*." (Dalam studi pengembangan, perolehan, atau adopsi senjata baru, sarana dan metode peperangan, pihak yang terikat kontrak tertinggi berkewajiban untuk menentukan apakah penggunaannya hanya untuk beberapa atau semua keadaan, dilarang oleh protokol ini atau oleh aturan hukum internasional lainnya yang berlaku untuk pihak yang mengadakan kontrak tinggi.)

[1] Iradhati Zhara dan Djajeng, *The Beginning of The International Law Applicattion to cyberattack : The status of Rule 30 Tallin Manual 1.0*, Vol 5, Universitas Padjajaran, 2021, h.

[2] Protokol Tambahan I Konvensi Jenewa 1977

Pasal tersebut menjelaskan bahwa penggunaan senjata baru termasuk menggunakan senjata *cyber* diwajibkan untuk mengikuti seluruh ketentuan pada hukum internasonal terkhususnya pada protokol tambahan tersebut. *Cyber attack* yang menyerang tanpa pandang bulu dan situasi kerap menjadi ancaman yang cukup signifikan bagi masyarakat sipil yang ingin menikmati layanan *cyber* yang dimilikinya.

Apabila dalam suatu kasus atau sengeketa tidak berkaitan langsung dengan sumber hukum humaniter internasional maka akan mengacu pada kalusula martenz. Klausula ini mencakup prinsip-prinsip yang dapat diterima dalam hukum kebiasaan, prinsip-prinsip kebiasaan dan prinsip hati nurani manusia. Isi klausula Martenz secara lengkap adalah sebagai berikut:[3] *Until a more complete code of laws of war is issued, the high contracting parties think it right to declare than it cases not include in the regulation adopted by them, population and belligerents remain und1er the protection and empire of the principle of international law, as they result from the usages estabilished beetwen civilized nation, from the laws of humanityand the ruquipment of the public conscience".* (Sampai suatu hukum perang yang lebih lengkap diterbitkan, pihak-pihak peserta agung berpendapat bahwa hal-hal yang tidak termuat dalam peraturan yang diadopsi mereka, penduduk dan pihak yang berperang tetap berada di bawah perlindungan dan imperium prinsip hukum internasional sebagai kebiasaan negara-negara beradab, dari hukum kemanusiaan dan hati nurani publik.)

Pada intinnya isi klausula diatas menjelaskan bahwa bilamana hukum humaniter internasional belum memiliki ketentuan terkait dengan kasus- kasus tertentu maka harus merujuk pada prinsip hukum internasional, prinsip pendapat umum, prinsip kemanusiaan, dalam Terdapat kasus *cyber attack* yang pernah terjadi akibat konflik antara Rusia dan Georgia. Carr dan Jefrrey menguraikannya dalam sebuah buku yang berjudul *inside cyber warfare* yang diluncurkan pada tahun 2010. Dalam buku tersebut menyampaikan bahwa Rusia mulai melakukan invasi pada wilayah Georgia pada 7 agustus 2008. Sebelumnya, Rusia bahkan telah menggunakan *cyber attack* pada website resmi pemerintahan milik Georgia. Ketika *cyber attak* yang dilakukan oleh Rusia, terdapat dua kelompok yang melakukan serangan terhadap infrastruktur atau *cyber space* milik Georgia yaitu, *Russian Bussiness Network* dan *StopGeorgia.ru*. Peluncuran serangan siber pertama kali ditujukan demi menghancurkan website resmi milik kepresidenanan Rusia melalui metode DDOS. Penggunaan *botnet* juga dilancarkan demi melumpuhkan website kepresidenan Georgia. *Shadowserver foundation* melakukan penelitian terhadap serangan yang dilancarkan tersebut. Mereka menyatakan bahwa "*machbot* merupakan varian *botnet* yang digunakan untuk menyerang website kepresidenan Rusia. *Bot* ini biasanya dimiliki oleh pihak Rusia" Serangan berikutnya diluncurkan pada website pemerintahan Georgia, misalnya saja website kementerian luar negeri Georgia yang pada akhirnya harus dipindahkan dalam bentuk blogspot.[4] Setelah kejadian ini, menteri luar negeri Georgia mengungkapkan kekesalannya dan menyampaikan bahwa Rusia telah sangat serius melakukan *cyber attack* terhadap website pemerintahan Georgia. Selanjutnya terjadi *cyber attack* terhadap website bank komersial terbesar di Georgia. Terdapat penelitian intensif yang dilakukan oleh salah seorang pengamat yang bernama Dancho Danchev, ia menyampaikan bahwa terdapat pembagian target serangan yang terpusat. Tanggal 11 Agustus 2008, Civil.ge menjadi target

[3] Pembukaan Konvensi Den Haag II 1899

[4] Carr, Jeffrey, *Inside Cyber Warfare*, O'Reilly, 2010, h. 15

serangan *cyber* berikutnya dengan metode serangan DDoS. Penyerangan sistem komputerisasi Rumah Sakit Daerah Zestafoni, Kutaisi, Sachkere dan Rumah Sakit rujukan Zudidi pada 16 hingga 19 Agustus 2008 yang membuat teknologi kesehatan dan alat medis digital terganggu atau tidak berfungsi. Hal ini berakibat pada penurunan kondisi pasien rawat inap pada masing-masing rumah sakit.

2. Metode Penelitian

Metode penelitian ini menggunakan tipe yuridis normatif dimana penelitian dilakukan dengan cara mengumpulkan data primer, sekunder dan tersier yang diperoleh menggunakan studi kepustakaan. Data yang telah terkumpul dianalisis secara kualitatif yang penguraiannya disusun secara sistematik berdasarkan disiplin ilmu hukum untuk mencapai kejelasan masalah yang akan dibahas.

3. Hasil Dan Pembahasan

3.1 Penerapan Hukum Humaniter Internasional Terhadap Pelanggaran *Cyber Attack*

Tanggung istilah *cyber space* pertama kali muncul saat dikemukakan oleh William Gibson pada 1984. Menurut William Gibson "*cyber space* merupakan suatu wadah yang menggabungkan berbagai elemen perangkat dan sistem jaringan yang digunakan untuk berkomunikasi dan berbagi informasi, istilah *cyber space* menurut terjemahan dari *freedictionary* adalah sebuah jaringan yang sifatnya global berbentuk suatu infrastruktur teknologi informasi dan saling terhubung antara satu dengan yang lain serta menjadi suatu tempat dimana komununikasi secara online terjadi."[5] *International telecomunication union* (ITU) dari *United Nation* menyatakan bahwa *cyber space* adalah "suatu medan baik yang secara fisik maupun non-fisik tercipta dari saling terhubungnya komputer, sistem komputer, network dan program komputer, data komputer, data konten, lalu lintas data, dan users atau pengguna."[6] Pengertian *cyber space* kemudian dipaparkan secara lebih lanjut oleh badan pertahanan Amerika Serikat sebagai "suatu ruang yang digunakan untuk melakukan segala bentuk komunikasi elektronik dan berbagi informasi serta segala bentuk urusan di dunia maya melalui jaringan komputer baik oleh pemerintah, masyarakat sipil maupun teroris."[7]

UNTERM mendifinisikan *cyber attack* sebagai "penggunaan sistem informasi untuk melakukan penyerangan dengan tujuan menghancurkan atau merusak sistem komputer, sistem informasi dan jaringan komputer musuh."[8] Hal ini dilakukan untuk mendapatkan keuntungan tersendiri bagi negara maupun individu baik keuntungan dari sisi militer maupun bisnis. ICRC juga mendefinisikan *cyber attack* sebagai "bentuk operasi terhadap musuh melalui sistem komputer dengan tujuan mengganggu, menghancurkan ataupu

---

[5] Andrew Muray D, *The Regulation of Cyberspace, Control in the Online Environment, Routledge-Cavendish*, London, h.5

[6] Even dkk, *Cyber Warfare: Concepts and Strategic Trends, Institute For National Security Studies*, 2012, h.10

[7] Steve Winterfield dan Jason Andreas, *The Basic of Cyber Warfare : Understanding the Fundamentals of Cyber Warfare in the Thery and Practice*, Syngress, Amsterdam, 2013, h. 16

[8] *UNTERM"Cyberwarfare",https://unterm.un.org/unterm/DGAACS/unterm.nsf/WebView/BFDE24673F1B1F6E85256 AFD006732A3?O*, diakses pada 18 Mei 2022

merusak."[9] Beranjak dari penjelasan diatas terkait dengan pengertian *cyber attack* maka merujuk pada suatu tindakan yang dilakukan oleh individu ataupun negara terhadap sistem jaringan komputer yang menimbulkan kerusakan dan terganggunya kegiatan komunikasi dan penyaluran informasi.

Penerapan Hukum Humaniter Internasional diatur berdasarkan tempat dimana konflik atau perang tersebut terjadi. Di wilayah laut, pengaturan yang terkait dengan perang terdapat pada konvensi yang dihasilkan melalui "konferensi Perdamaian II di Den Haag seperti konvensi VI tentang Status Kapal Dagang Musuh pada saat Permulaan Peperangan, konvensi IX tentang Pemboman oleh Angkatan Laut di Waktu Perang, dan konvensi XIII tentang Hak dan Kewajiban Negara Netral dalam Perang di Laut"[10], Pasal 2 ayat 4 Piagam PBB, menjelaskan bahwa:[11] *All members shall refrain in their international relations from the threat or use of force a the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations*. (Seluruh anggota wajin menahan diri pada hubungan internasional mereka dari ancaman ataupun penggunaan kekerasan terhadap kemerdekaan politik atau integritas territorial setiap negara, atau dengan cara lain tidak konsisten pada Tujuan Perserikatan Bangsa-Bangsa).

Pasal tersebut menjelaskan tentang *territorial integrity*, suatu negara menggunakan angkatan bersenjata miliknya baik di udara, laut dan darat wajib didasarkan pada kedaulatan milik negara tersebut. Sama halnya jika berbicara terkait dengan *cyber space,* harus ada penentuan terkait dengan batas teritori atau batas maupun cakupan dari *cyber space* itu sendiri.

Michael Schmitt memaparkan setidaknya ada 5 kriteria yang harus dipenuhi untuk menyatakan *cyber attack* merupakan suatu serangan bersenjata dengan pendekatan kasus *cyber attack* Rusia ke Georgia. Kriteria yang pertama adalah *severity.* Maksud dari *severity* sendiri adalah bahwa :[12] Serangan siber menghancurkan sistem jaringan dan kompter serta infrastuktur yang telah terkomputerisasi atau yang termasuk kategori infrastruktur vital seperti lampu lalu lintas, bendungan, pembangkit listrik, infrastruktur telekomunikasi dan infrastruktur medis. Hal-hal tersebut secara tidak langsung menimbulkan kekacauan dan mengganggu aktivitas masyarakat bahkan kematian karena tidak adanya komunikasi, tidak adanya listrik, tidak adanya ketersediaan air dan yang paling parah adalah tidak adanya pertolongan medis menggunakan peralatan canggih kepada pasien yang sedang kritis.

Berbagai analisis mengenai efek-efek dari *cyber attack* tersebut, sama dengan apa yang terjadi pada kasus *cyber attack* yang dilancarkan oleh Rusia terhadap Georgia pada tahun 2008. Serangan *cyber* yang dilancarkan ditujukan untuk melumpuhkan website Presiden Georgia, komersial bank, kementerian luar negeri, bahkan website umum yang juga diakses oleh masyarakat sipil (*www.president.gov.ge*) serta rumah sakit daerah dengan menggunakan *distributed denial of service* Berdasarkan penjelasan diatas patutlah bila *cyber*

[9] ICRC, *The Evolution of Warfare*, Internationl Review of the Red Cross, ICRC Vol. 97, No.900,2015, p.147
[10] *http://ninapramudia-fisipq17.web.unair.ac.id,*diakses pada 19 Mei 2022
[11] Piagam PBB Pasal 2 Ayat 4
[12] MP Ferreira-Snyman, 2006, *The Evolution of State Sovereignty: A Historical* Overview, University of Leyden Netherland, h. 9

attack dikatakan memenuhi kriteria ini karena telah menggunakan metode DDoS untuk melumpuhkan sistem komputer termasuk infrastruktur yang terkomputerisasi seperti website dan jaringan pada rumah sakit.

Kriteria berikutnya adalah *immediacy*. Maksud dari *immediacy* sendiri adalah bahwa terdapat dampak panjang yang dialami oleh negara yang menjadi korban. *Immediacy*. Jika melihat pada dampak panjang yang dialami negara yang menjadi korban serangan, maka negara yang terkena serangan siber juga mengalami hal yang sama. Jika virus, *worm* dan *Trojan* sudah masuk kedalam sistem komputer, maka akan terinfeksi pada saat komputer tersebut menyala. file dan program yang terdapat dalam akan mengalami kekacauan dan kinerja komputer mengalami kekacauan. Adanya jumlah waktu dari *cyber attack* untuk bertahan dan durasi lama yang dibutuhkan agar efek tersebut dapat dirasakan. [13] Penyerangan bertubi – tubi oleh Rusia ke Georgia bertahan selama 21 hari. Dimulai dari tanggal 7 Agustus 2008 hingga 28 Agustus 2008. Efek dari penyerangan tersebut mulai berhenti ketika tim *cyber* pemerintah Georgia berhasil mematahkan atau melumpuhkan virus yang telah menguasai sistem jaringan yang telah terkomputerisasi tersebut. Berdasarkan pada penjelasan diatas maka *cyber attack* memenuhi kriteria ini karena telah menimbulkan dampak yang panjang dan berhenti ketika telah ditangani dengan intensif.

Kriteria berikutnya adalah *Directness* yang bermaksud bahwa "efek yang ditimbulkan dari adanya *cyber attack* dapat merugikan, dimana kegagalan fungsi organ tubuh karena gangguan pada alat atau teknologi medis mengawali timbulnya *incidental loss of life* atau korban jiwa."[14] Penyerangan sistem komputerisasi Rumah Sakit Daerah Zestafoni, Kutaisi, Sachkere dan Rumah Sakit rujukan Zudidi pada 16 hingga 19 Agustus 2008 yang membuat teknologi kesehatan dan alat medis digital terganggu atau tidak berfungsi. Hal ini berakibat pada penurunan kondisi pasien rawat inap pada masing-masing rumah sakit. Bahkan, tercatat sekitar 28 pasien yang berada dalam keadan kesehatan darurat tidak mendapatkan pertolongan intensif dan membuat 32 pasien dengan kondisi kritis harus kehilangan nyawa. Hal ini tentu saja berdampak terhadap pemberian pelayanan oleh rumah sakit kepada masyarakat karena setiap orang wajib untuk mendapatkan pelayanan yang baik atas kesehatan[15]. Berdasarkan penjelasan diatas, maka *cyber attack* memenuhi kriteria ini karena terdapat beberapa korban jiwa yang berakibat dari penyerangan ini.

Selanjutnya terdapat kriteria *Invasiveness*. Menurut Schmitt, "serangan invansi secara fisik melintasi perbatasan negara atau secara elektronik melewati batas cakupan atau jangkauan *cyber* milik suatu negara."[16] Rusia berhasil masuk ke dalam jaringan sistem informasi digital milik pemerintah Georgia, Bank Komersial dan sistem komputerisasi rumah sakit daerah dan rumah sakit rujukan. Hal ini berarti Rusia telah melanggar batas kedaulatan *cyber* milik negara Georgia. Berdasarkan penjelasan diatas maka *cyber attack* memenuhi kriteria ini karena Rusia secara jelas telah masuk dan mengganggu infrastruktur *cyber space* negara Georgia.

---

[13] *Ibid,* h. 10

[14] *Ibid*, h. 10

[15] Rehatta, V. J. B., Leatemia, W., & Palijama, T. (2021). *Fulfillment of Children's Health Rights in Ambon City During The Covid 19 Pandemic*. *SASI*, *27*(2), 187-195.

[16] *Ibid,* h. 10

Kriteria terakhir adalah *Presumptive legitimacy.* Menurut Schmitt, "kurang diterimanya *cyber attack* berdasarkan praktik negara-negara (*states practice*), memperkuat bukti bahwa, *cyber attack* adalah *illegal use of force or an armed attack*."[17] Pemerintah Georgia menuding bahwa serangan siber Rusia telah melewati batas-batas kemanusian karena telah mengganggu aktivitas masyarakat sipil dan bahkan teknologi kesehatan yang sangat diperlukan oleh pasien-pasien pada rumah sakit daerah dan rujukan. Beberapa negara seperti Prancis, Inggris, Amerika dan Jerman juga telah mengambil sikap untuk mengutuk keras invasi Rusia ke Georgia termasuk pada serangan siber yang dilakukan negara Rusia tersebut.

3.2 Tanggung Jawab Negara Berdasarkan Hukum Internasional

Tanggung jawab negara menjadi bagian yang tidak terlepas pisahkan dari setiap perbuatan atau tindakan suatu negara terhadap negara lain. Sebelum masuk pada penjelesan mengenai pengertian tanggungjawab negara, maka perlu dijelaskan pula pengertian dari pertanggungjawaban itu sendiri. Menurut kamus besar bahasa Indonesia, "tanggungjawab diartikan sebagai suatu kondisi atau keadaan untuk menanggung segala sesuatunya."[18] Menanggung dalam hal ini diartikan sebagai menanggung atas akibat yang dilakukan atau diperbuat baik itu merupakan kelalaian maupun kesalahan. Sugeng istianto berpendapat bahwa pertanggungjawaban merujuk pada kewajiban untuk memberikan suatu jawaban dan pemulihan atas semua dampak yang berakibat kerugian yang timbul.[19] "Pertanggungjawaban berarti kewajiban memberikan jawaban yang merupakan perhitungan atas suatu hal yang terjadi, dan kewajiban untuk memberikan pemulihan atas kerugian yang mungkin ditimbulkannya."[20]

Tanggung jawab negara diartikan pula sebagai kewajiban yang harus dijalankan oleh suatu negara kepada negara lain berdasarkan perintah dan mekanisme yang telah diatur didalam hukum internasional. [21] Tanggungjawab negara dalam hukum internasional merupakan suatu prinsip dalam hukum internasional yang didalamnya mengatur terkait dengan kesalahan maupun kelalaian suatu negara yang memicu terjadinya dampak negatif bagi negara lain. Pertanggung jawaban negara dalam hukum internasional, pada dasarnya dilatarbelakangi oleh pemikiran bahwa tidak ada negara manapun di dunia ini yang dapat menikmati hak-haknya tanpa menghormati hak-hak negara lain[22].

"Hukum tentang tanggung jawab negara adalah hukum mengenai kewajiban negara yang timbul manakala negara telah atau tidak melakukan suatu tindakan."[23] Intinya bahwa, suatu kesalahan yang dibuat oleh negara yang dampaknya dirasakan pula oleh negara lain dapat menimbulkan tanggung jawab negara ataupun dikenal juga dengan istilah kewajiban negara untuk memperbaiki atau memulihkan sesuatu agar menjadi seperti semula.

---

[17] *Ibid, hal* 12

[18] Waridah Ernawati, *Kamus Besar Bahasa Indonesia*, Bmedia, Jakarta, 2017

[19] F. Soegeng Istanto, *Hukum Internasional*, UAJ Yogyakarta, Yogyakarta, 1994, h.77

[20] D.J. Harris, *Cases and Materials on International Law*, Sweet and Maxwell, London, 1982, h. 374

[21] Rebecca M.M. Wallace, *International Law*, Fourth Edition, Sweet and Maxwell, London, 2002, h. 175

[22] Papilaya, B. D. A., Peilouw, J. S. F., & Waas, R. M. (2021). Tanggung Jawab Negara Terhadap Pelanggaran Hak Asasi Manusia Di Belarusia Ditinjau Dari Hukum Internasional. *TATOHI: Jurnal Ilmu Hukum*, *1*(6), 531-545.

[23] Ridwan H.R., *Hukum Administrasi Negara*, Raja Grafindo Persada, Jakarta, 2006, h. 335-337

Terdapat beberapa unsur-unsur pertanggungjawaban negara. Shaw berpendapat bahwa karakteristik yang menjadi unsur timbulnya tanggungjawab negara ini dipengaruhi oleh beberapa faktor:

1) Adanya kewajiban berdasarkan hukum dan prinsip internasional umum
2) Adanya kelalaian dan kesalahan yang dilakukan melanggar hukum dan prinsip internasional
3) Adanya dampak berupa kerusakan maupun kerugian terhadap suatu negara.

Penjelasan diatas berkaitan dengan unsur-unsur apa saja yang harus dipenuhi untuk memicu timbulnya tanggungjawab negara. Pertama, adanya kewajiban berdasarkan hukum dan prinsip internasional umum, artinya bahwa kewajiban atau tanggungjawab yang timbul haruslah sesuai dengan ketentuan yang diatur di dalam hukum internasional ataupun menjadi suatu pedoman kehidupan internasional yang merupakan bagian dari prinsip hukum internasional. Kedua, harus ada kesalahan baik disengaja ataupun kealpaan yang merupakan bagian inti yang mengukur apakah perbuatan tersebut harus dipertanggungjawabkan ataukah tidak. Ketiga, dari kesalahan negara tersebut menimbulkan dampak berupa kerugian maupun kerusakan pada negara lainnya. Jadi, negara lain punya hak untuk menuntut atas dampak negatif yang diperoleh akibat perbuatan negara.

3.3 Tanggung Jawab Negara Terhadap Penggunaan *Cyber Attack* Berdasarkan Hukum Internasional

Tanggung jawab negara atau tanggung jawab internasional diperuntukan bagi setiap negara yang melakukan tindakan berupa kelalaian maupun kesalahan yang bertentangan dengan prinsip dan pengaturan hukum internasional yang berlaku.[24] Seperti penjelasan pada bab sebelumnya, telah membuktikan bahwa tindakan *cyber attack* yang dilakukan oleh suatu negara kepada negara lain merupakan tindakan yang bertentangan dengan prinsip hukum internasional dan memenuhi unsur sebagai domain perang baru serta bentuk serangannya memenuhi persyaratan serangan dalam konteks konflik bersenjata.

Bentuk tanggung jawab negara berdasarkan *articles on state responbility* berupa penghentian dan tidak terulangi serta reparasi yang diberikan oleh negara penyerang kepada negara korban. Pada pasal 30 *articles on state responbility* menjelaskan bahwa "Negara yang bertanggung jawab atas tindakan yang salah secara internasional berkewajiban: (a) untuk menghentikan tindakan itu, jika tindakan itu berlanjut; (b) untuk menawarkan jaminan dan jaminan yang tepat untuk tidak mengulangi, jika keadaan mengharuskan demikian."[25]

Berkaitan dengan *cyber attack*, maka negara penyerang wajib untuk menghentikan segala bentuk serangan baik menggunakan *malware, distributed denial of service* maupun *botnet* kepada negara korban. Penghentian dilakukan sesegera mungkin agar tidak menimbulkan dampak yang lebih parah dan menimbulkan banyak orang serta objek yang terganggu maupun dirugikan.

[24] *Articles on State Responbility*
[25] *Articles on state responbility,* pasal 30

Pada pasal 31 *articles on state responbility* menyebutkan bahwa:

1) Negara yang bertanggung jawab berkewajiban untuk melakukan reparasi penuh atas kerugian yang disebabkan oleh tindakan yang salah secara internasional.
2) 2. Cedera meliputi segala kerusakan, baik material maupun moral, yang disebabkan oleh tindakan salah suatu negara secara internasional."[26]

Intinya, bahwa negara penyerang berkewajiban untuk melakukan perbaikan atas segala bentuk kerusakan dan gangguan yang ada akibat dari *cyber attack* yang dilancarkan. Biasanya, kerusakan atau gangguan terjadi pada alat elektronik da sistem jaringan negara korban. Hal inilah yang menjadi objek perbaikan secara menyeluruh agar sistem jaringan yang menggunakan teknologi informasi dan komunikasi dapat kembali stabil.

Sesuai dengan ketentuan pasal 34 *articles on state responbility*, bentuk-bentuk reparasi atau perbaikan adalah berupa restitusi, kompensasi dan kepuasan. Restitusi diatur pada pasal 35 *articles on state responbility* yang berbunyi: "Suatu negara yang bertanggung jawab atas suatu tindakan yang salah secara internasional berkewajiban untuk melakukan restitusi, yaitu untuk mengembalikan situasi yang ada sebelum tindakan yang salah itu dilakukan, asalkan dan sejauh restitusi: a) tidak secara materi tidak mungkin; b) tidak melibatkan beban di luar proporsi keuntungan yang diperoleh dari restitusi dan bukan kompensasi."[27]

Intinya bahwa restitusi dilakukan hanya untuk mengembalikan keadaan menjadi pulih seperti sedia kala. Restitusi dilakukan dengan proporsi yang sesuai dengan kerusakan sistem jaringan yang ada. Restitusi tidak dilakukan untuk membuat keaadan lebih baik dari sebelumnya (sebelum penyerangan) dan tidak keluar dari tanggungan beban yang proporsinya telah sesuai dengan besaran kerusakan akibat *cyber attack* yang terjadi.

Kompensasi diatur pada pasal 35 *Articles on State Responbility* yang berbunyi:

1) Negara yang bertanggung jawab atas suatu tindakan yang salah secara internasional berkewajiban untuk mengganti kerugian yang diakibatkannya, sejauh kerusakan tersebut tidak diperbaiki dengan restitusi.
2) Kompensasi harus mencakup kerugian yang dapat dinilai secara finansial termasuk hilangnya keuntungan sejauh hal itu ditetapkan.[28]

Apabila restitusi tidak mampu untuk menjawab segala bentuk objek yang harus diperbaiki karena misalnya sudah tidak bisa lagi untuk diperbaiki melainkan diperbaharui maka kompensasi hadir untuk menjawab masalah tersebut dan tanggungan tersebut dapat dinilai secara finansial. Selanjutnya adalah dalam bentuk memberikan kepuasan, pada pasal 37 menyebutkan bahwa: 1) Negara yang bertanggung jawab atas suatu tindakan yang salah secara internasional berkewajiban untuk memberikan kepuasan atas kerugian yang diakibatkan oleh tindakan tersebut sepanjang tidak dapat diperbaiki dengan restitusi atau kompensasi; 2). Kepuasan dapat berupa pengakuan atas pelanggaran, ekspresi penyesalan, permintaan maaf formal atau modalitas lain yang sesuai; 3) Kepuasan tidak boleh melebihi

[26] *Articles on state responbility,* pasal 31
[27] *Articles on State Responbility*, Pasal 35
[28] *Articles on State Responbility,* Pasal 36

kerugian dan tidak boleh dalam bentuk yang mempermalukan negara yang bertanggung jawab."[29]

Negara penyerang dapat mengakui kesalahan atas pelanggaran berupa tindakan *cyber attack* yang telah mengganggu sistem jaringan dan melumpuhkan aktivitas teknologi informasi pemerintah maupun masyarakat suatu negara. Pengakuan disertai permohonan maaf diselingi penyesalan dapat dipublikasi baik melalui suatu surat pernyataan maupun secara langsung melalui konferensi pers. Intinya bahwa pernyataan yang dikeluarkan dapat memuaskan negara korban *cyber attack* namun tidak boleh berlebihan dan mempermalukan negara yang bertanggung jawab.

4. Kesimpulan

Tanggung jawab negara atau tanggung jawab internasional diperuntukan bagi setiap negara yang melakukan tindakan berupa kelalaian maupun kesalahan yang bertentangan dengan prinsip dan pengaturan hukum internasional yang berlaku.[30] Seperti penjelasan pada bab sebelumnya, telah membuktikan bahwa tindakan *cyber attack* yang dilakukan oleh suatu negara kepada negara lain merupakan tindakan yang bertentangan dengan prinsip hukum internasional dan memenuhi unsur sebagai domain perang baru serta bentuk serangannya memenuhi persyaratan serangan dalam konteks konflik bersenjata. Bentuk tanggung jawab negara berdasarkan *articles on state responbility* berupa penghentian dan tidak terulangi serta reparasi yang diberikan oleh negara penyerang kepada negara korban. Berkaitan dengan *cyber attack*, maka negara penyerang wajib untuk menghentikan segala bentuk serangan baik menggunakan *malware, distributed denial of service* maupun *botnet* kepada negara korban. Penghentian dilakukan sesegera mungkin agar tidak menimbulkan dampak yang lebih parah dan menimbulkan banyak orang serta objek yang terganggu maupun dirugikan. Negara penyerang dapat mengakui kesalahan atas pelanggaran berupa tindakan *cyber attack* yang telah mengganggu sistem jaringan dan melumpuhkan aktivitas teknologi informasi pemerintah maupun masyarakat suatu negara. Pengakuan disertai permohonan maaf diselingi penyesalan dapat dipublikasi baik melalui suatu surat pernyataan maupun secara langsung melalui konferensi pers. Intinya bahwa pernyataan yang dikeluarkan dapat memuaskan negara korban *cyber attack* namun tidak boleh berlebihan dan mempermalukan negara yang bertanggung jawab.

Daftar Referensi

Andrew Muray D, *The Regulation of Cyberspace, Control in the Online Environment, Routledge-Cavendish*, London

Carr, Jeffrey, *Inside Cyber Warfare*, O'Reilly, 2010.

D.J. Harris,(1982) *Cases and Materials on International Law*, Sweet and Maxwell, London

Even dkk (2012), Cyber Warfare: Concepts and Strategic Trends, Institute For National Security Studies

[29] *Articles on State Responbility*, Pasal 37
[30] *Articles on State Responbility*

F. Soegeng Istanto (1994), *Hukum Internasional*, UAJ Yogyakarta, Yogyakarta

Steve Winterfield dan Jason Andreas, The Basic of Cyber Warfare : Understanding the Fundamentals of Cyber Warfare in the Thery and Practice, Syngress, Amsterdam, 2013.

ICRC,(2015) *The Evolution of Warfare*, Internationl Review of the Red Cross, ICRC Vol. 97, No.900

Iradhati Zhara dan Djajeng,(2021), *The Beginning of The International Law Applicattion to cyberattack : The status of Rule 30 Tallin Manual 1.0*, Vol 5, Universitas Padjajaran

MP Ferreira-Snyman (2006), *The Evolution of State Sovereignty: A Historical* Overview, University of Leyden Netherland.

Papilaya, B. D. A., Peilouw, J. S. F., & Waas, R. M. (2021). *Tanggung Jawab Negara Terhadap Pelanggaran Hak Asasi Manusia Di Belarusia Ditinjau Dari Hukum Internasional*. *TATOHI: Jurnal Ilmu Hukum*, *1*(6), 531-545.

Rehatta, V. J. B., Leatemia, W., & Palijama, T. (2021). *Fulfillment of Children's Health Rights in Ambon City During The Covid 19 Pandemic*. *SASI*, *27*(2), 187-195.