Hukum

ANALISIS PENGGUNAAN MEDIA SIBER UNTUK *SELF DEFENSE* DALAM *CYBER WARFARE* DITINJAU DARI HUKUM INTERNASIONAL

Rifqi Fatkurrahman*, Go Lisanawati, Marlina Br Purba

Fakultas Hukum Universitas Surabaya, Raya Kalirungkut, Surabaya 60293

**Corresponding author:* rifqifatkurrahman@gmail.com

Abstract–*Cyber warfare is a term that refers to conflicts carried out in cyberspace using cyber media as a weapon. Cyber warfare includes state actions not only in carrying out attacks, but also in carrying out actions to defend itself. The cyber warfare that occurred between Russia and Georgia in 2008 was a cyber war that used cyber media to attack and defend. Georgia counterattacked using cyber media to defend itself from Russian cyber attacks. International law regulates state actions in self-defense based on Article 51 of the UN Charter which requires armed attack, the necessity and proportionalities in its implementation. In international law, there are no regulations regarding a country's self-defense measures when cyber warfare occurs. This causes Article 51 of the UN Charter to also apply to cyber warfare. In international law, there are no regulations regarding a country's self-defense actions when cyber war occurs. This causes Article 51 of the UN Charter to also apply to cyber warfare. This research aims to analyze whether Georgia's actions in carrying out retaliatory attacks in response to Russian cyberattacks can be categorized as acts of self-defense under international law. The research method used is the normative juridical legal research method, namely a legal research method by solving legal facts/events using international legal sources. The results of this research indicate that Georgia's use of cyber media as a counterattack to defend itself from Russian cyber attacks cannot be categorized as an act of self-defense based on Article 51 of the UN Charter and customary international law. Even though it cannot be categorized as a form of self-defense, Russia's actions in carrying out its cyber attacks still had a significant impact on Georgia.*

Keywords: *cyber warfare, self defense, armed attack*

Abstrak–Peperangan siber adalah suatu istilah yang merujuk pada konflik yang dilakukan di ruang siber dengan menggunakan media siber sebagai senjatanya. Peperangan siber di dalamnya mencakup tindakan negara tidak hanya dalam melakukan serangan, namun juga dalam melakukan tindakan untuk bertahan atau mempertahankan diri. Perang siber yang terjadi antara Rusia dan Georgia pada tahun 2008 di dalamnya mencakup penggunaan media siber yang ditujukan untuk menyerang dan bertahan. Georgia melakukan serangan balasan menggunakan media siber untuk mempertahankan diri terhadap serangan siber Rusia. Hukum internasional di dalamnya mengatur mengenai tindakan negara untuk mempertahankan diri berdasarkan pada *Article 51 UN Charter* yang mengharuskan adanya serangan bersenjata, keharusan dan kesebandingan dalam pelaksanaannya. Belum adanya ketentuan khusus dalam hukum internasional yang mengatur mengenai perang siber, membuat pengaturan mengenai tindakan mempertahankan diri bagi suatu negara selama perang siber juga turut di dasarkan pada *Article 51 UN Charter.* Penelitian ini bertujuan untuk menganalisa apakah tindakan Georgia dalam melakukan serangan balasan untuk merespons serangan siber Rusia dapat dikategorikan sebagai tindakan membela diri berdasarkan pada hukum internasional. Metode penelitian yang digunakan adalah menggunakan metode penelitian hukum yuridis normatif, yaitu metode penelitian hukum dengan memecahkan fakta/peristiwa hukum menggunakan sumber-sumber hukum internasional. Hasil dari penelitian ini menunjukkan bahwa penggunaan media siber yang digunakan oleh Georgia sebagai serangan balasan untuk mempertahankan diri dari serangan siber Rusia tidak dapat dikategorikan sebagai tindakan *self defense* berdasarkan *Article 51 UN Charter* dan hukum kebiasaan internasional. Namun, meskipun tidak dapat dikategorikan sebagai suatu bentuk *self defense,* perbuatan Rusia dalam melakukan serangan sibernya tetap memiliki dampak yang cukup signifikan terhadap Georgia.

Kata kunci: *perang siber, hak bela diri, dan serangan bersenjata*

Pendahuluan

Perkembangan yang terus terjadi dari zaman ke zaman telah memberikan banyak perubahan pada kehidupan manusia. Salah satu bentuk perkembangan tersebut adalah dengan adanya dunia maya *(cyberspace),* yang menggeser zaman ke arah modernisasi dengan mempengaruhi kehidupan manusia dan memberikan beragam efek positif dalam kehidupan bermasyarakat. Namun, kemajuan tersebut tidak dapat hanya dipandang sebagai suatu kemajuan yang memiliki dampak positif saja. Seiring dengan semakin berkembangnya teknologi, informasi, dan komunikasi, terdapat pula suatu metode baru atau cara-cara baru yang dikembangkan untuk

melakukan kejahatan dalam *cyberspace* bahkan hingga suatu metode baru dalam melakukan peperangan menggunakan media teknologi internet atau komputer yang dapat juga disebut sebagai *cyber warfare*.

United Nations Interregional Crime and Justice Research Institute (UNICRI) mengartikan *cyber warfare* sebagai suatu tindakan yang ditujukan untuk mengganggu jaringan internet atau komputer dari negara lain dengan maksud untuk menyebabkan kerusakan (Tampubolon, 2019). Senjata yang digunakan dalam *cyber warfare* adalah berupa media siber yang merupakan suatu perangkat lunak atau kode yang dirancang dan digunakan untuk melancarkan serangan siber. Penggunaan media siber yang digunakan untuk menyerang *(cyber attack)*, tentunya menyebabkan pula adanya perubahan dan menciptakan pula berbagai tindakan negara yang salah satunya adalah untuk bertahan dan mempertahankan diri *(self defense)*.

Salah satu kasus yang berkaitan dengan *cyber warfare* dan penggunaan media siber untuk menyerang dan bertahan adalah pada kasus yang terjadi antara Rusia dan Georgia pada tahun 2008 (Carr, 2009). *Cyber warfare* tersebut terjadi selama konflik militer antara kedua negara yang bermula ketika Georgia mengklaim wilayah Ossetia Selatan yang didukung oleh Rusia sehingga pada akhirnya berujung pada intervensi militer Rusia di Georgia. Selama konflik tersebut Rusia terus melakukan serangan siber menggunakan berbagai metode seperti*, Distributed Denial of Services (DDoS)* dan *site defacement* yang ditujukan untuk mengganggu jaringan internet, server dan memprovokasi masyarakat sipil di wilayah Georgia. Atas tindakan Rusia dalam melakukan serangan siber tersebut, Georgia kemudian merespons dengan melakukan serangan siber yang dianggapnya sebagai bentuk pembelaan diri *(self defense)* terhadap perusahaan media milik Ossetia Selatan dan Rusia untuk menghentikan serangan tersebut (Markoff, 2008).

Hukum Internasional di dalamnya memuat ketentuan-ketentuan yang ditujukan untuk menjaga hubungan internasional agar tetap aman dan damai. Suatu negara dilarang mengancam atau menggunakan kekuatan bersenjata terhadap negara lain dan sebaliknya untuk menghadapi serangan bersenjata yang dilakukan oleh suatu negara, negara diperbolehkan untuk menggunakan kekuatan bersenjata sebagai upaya untuk membela diri *(self defense)* sebagaimana diatur dalam ketentuan *Article 51 United Nations Charter (UN Charter)*.

Article 51 UN Charter di dalamnya menyatakan bahwa Hak pembelaan diri *(self defense)* merupakan suatu upaya yang dapat dilakukan apabila terdapat serangan bersenjata terhadap suatu negara anggota PBB yang dapat dilakukan secara individual atau bersama-sama antara suatu negara dengan negara lain. Hak pembelaan diri *(self defense)* sejauh dibutuhkan sebagai tindakan yang sah untuk mencegah atau menangkis serangan bersenjata harus pula disertai dengan batasan-batasan tertentu agar tindakan pembelaan diri tersebut tidak mengakibatkan kerugian yang tidak sebanding atas serangan yang dilakukan. Maka, perlu untuk dilakukan analisis hukum terhadap penggunaan media siber untuk *self defense* dalam *cyber warfare* mengingat belum adanya aturan yang khusus mengatur mengenai *cyber warfare* dan dampak yang dapat ditimbulkan atas adanya serangan media siber tersebut tidak lagi dapat membedakan siapa targetnya, sehingga dapat berpengaruh pula terhadap penduduk maupun objek sipil dalam konflik bersenjata, khususnya penggunaan media siber dalam kasus *cyber warfare* antara Rusia dengan Georgia pada tahun 2008.

Berdasarkan latar belakang yang telah dipaparkan di atas, ditemukan suatu permasalahan yaitu, "Apakah penggunaan media siber yang dilakukan oleh Georgia sebagai respons atas serangan siber Rusia dapat dikategorikan sebagai *self defense* dalam *cyber warfare* berdasarkan hukum internasional?

Metode Penelitian

Metode penelitian yang digunakan dalam penulisan hukum ini adalah metode penelitian yuridis normatif, yaitu penelitian hukum dengan cara memecahkan fakta/peristiwa hukum dengan menggunakan norma dan prinsip hukum dalam konvensi-konvensi hukum internasional atau asas, prinsip, konsep/pendapat ahli melalui literatur yang bersangkutan dengan hukum internasional.

Dilakukannya penelitian ini bertujuan untuk menganalisa penggunaan media siber bagi Georgia untuk *self defense* sebagai respons atas serangan siber Rusia Pada tahun 2008. Pendekatan masalah yang digunakan dalam penelitian ini adalah pendekatan secara *statute Approach* dan *conceptual Approach.* Pendekatan secara *statute Approach* merupakan pendekatan yang dilakukan dengan mengidentifikasi setiap konvensi-konvensi Internasional yang berkaitan dengan materi yang sedang dibahas. Pendekatan *conceptual Approach* merupakan suatu pendekatan yang dilakukan dengan cara membahas dan mengidentifikasi pandangan serta pendapat dari para pakar hukum sebagai pendukung argumentasi untuk menyelesaikan materi yang dibahas.

Bahan hukum yang digunakan dalam penelitian ini meliputi bahan hukum primer yang berupa sumber-sumber berupa aturan hukum yang berupa konvensi-konvensi internasional, dan perjanjian-perjanjian bilateral maupun multilateral, yaitu *Charter of the United Nations* (Piagam Perserikatan Bangsa-Bangsa), Konvensi Jenewa 1949 *(Geneva Conventions)*, Protokol tambahan I Konvensi Jenewa 1949, dan ketentuan-ketentuan yang berhubungan dengan penggunaan media siber untuk keperluan *self defense* dalam konflik *cyber warfare* antar negara. Bahan hukum sekunder, yaitu bahan hukum yang memberikan tambahan informasi dan penjelasan terkait dengan bahan hukum primer seperti buku-buku yang terkait dengan penelitian, dokumen-dokumen internasional maupun nasional, artikel atau jurnal, dan karya ilmiah lainnya.

Kronologi Kasus

Kasus *cyber warfare* antara Rusia dan Georgia pada tahun 2008 merupakan salah satu peristiwa penting dalam perkembangan *cyber warfare.* Peristiwa tersebut menandai penggunaan media siber untuk serangan dan pertahanan diri untuk pertama kalinya oleh sebuah negara. Kasus tersebut bermula ketika Rusia mendukung wilayah Abkhazia dan Ossetia Selatan dalam upayanya untuk memerdekakan diri dari Georgia, sedangkan Georgia berusaha untuk mempertahankan wilayah-wilayah yang mencoba untuk memisahkan diri tersebut. Pada 20 Juli 2008 Rusia sudah mulai menyerang Georgia melalui serangan-serangan siber *(cyber attack)* yang ditujukan terhadap website-website pemerintahan Georgia. Serangan tersebut menyebabkan Georgia melakukan serangkaian tindakan yang dianggapnya sebagai bentuk pembelaan. Pada tanggal 5 Agustus 2008, Georgia melakukan serangan siber terhadap dua situs yakni situs website OSInform News Agency dan OSRadio yang dilakukan sebagai tanggapan terhadap serangan siber Rusia sejak bulan Juli (Kiyuna & Conyers, 2015).

Setelah kejadian tersebut, pada tanggal 7 hingga 9 Agustus 2008 serangan siber secara besar-besaran kemudian kembali dilancarkan oleh Rusia terhadap situs-situs milik Georgia. Serangan siber Rusia tersebut diketahui berasal dari salah satu organisasi yang disebut sebagai *Russian Business Network (RBN)* (Carr, 2009). Georgia dalam menanggapi serangan tersebut kemudian melancarkan serangan siber terhadap salah satu kantor berita milik Rusia, *RIA Novosti* pada tanggal 10 Agustus 2008. Serangan Rusia kemudian masih berlanjut pada tanggal 11 Agustus 2008 dengan mengubah tampilan situs Georgia yang memperlihatkan wajah Presiden ke-3 Georgia, Mikheil Saakashvili dengan Adolf Hitler. Serangan dengan metode propaganda siber oleh Rusia kemudian mulai dilancarkan melalui forum *StopGeorgia.ru* pada tanggal 12 Agustus 2008. Serangan-serangan tersebut terus berlanjut hingga akhirnya para pihak yang berkonflik sepakat untuk melakukan gencatan senjata pada tanggal 14 Agustus 2008.

Analisis Kasus

Menurut *Article 51 UN Charter,* hak untuk membela diri *(self defense)* merupakan hak yang memberikan legalitas bagi suatu negara untuk menggunakan kekuatan bersenjata sebagai upaya pembelaan diri apabila mendapatkan serangan bersenjata dari subjek hukum internasional lainnya. Sebelum suatu negara dibenarkan untuk menggunakan haknya dalam membela diri, maka terlebih dahulu harus dibuktikan bahwa terdapat adanya serangan bersenjata *(armed attack)* yang ditujukan terhadap negara tersebut, termasuk dalam kasus *cyber warfare* yang dilakukan oleh Rusia terhadap

Georgia. Serangan balasan untuk membela diri kemudian harus dilakukan dengan didasarkan pada dua kriteria utama yang telah menjadi hukum kebiasaan internasional dalam penerapan *self defense* sebagai acuan untuk menentukan batasan-batasan tertentu dalam melakukan tindakan balasan terhadap negara penyerang. Kriteria-kriteria tersebut meliputi *necessity* (kebutuhan) dan *proportionality* (kesebandingan).

Serangan bersenjata *(armed attack)* sebagai salah satu syarat utama dapat dilakukannya *self defense,* menurut *International Law Commission* merupakan serangan yang telah dilaksanakan oleh suatu negara untuk menyerang negara lain dengan mempertimbangkan skala dan efek yang ditimbulkannya. Sejalan dengan pernyataan tersebut, pada *Rule 13 (5) Tallinn Manual* disebutkan bahwa serangan bersenjata merupakan istilah yang mengandaikan penggunaan kekerasan yang melebihi ambang batas skala dan dampak yang ditimbulkan sebagaimana diatur dalam *Article 2 (4) UN Charter*. Berdasarkan pada hal tersebut, maka serangan bersenjata dalam hukum internasional dapat diartikan sebagai serangan yang mencakup tindakan kekerasan hingga menyebabkan cedera atau kematian pada orang atau kerusakan terhadap benda/objek secara fisik.

Secara umum serangan siber tidak menyebabkan adanya kerusakan terhadap objek/benda secara langsung. *Rule 13 Tallinn Manual (9)* di dalamnya kemudian menegaskan bahwa kriteria skala dan efek tanpa adanya kematian, cedera, atau kerusakan fisik secara langsung dalam serangan *cyber warfare* dapat dianggap sebagai serangan bersenjata berkaitan dengan adanya serangan terhadap *"critical infrastructures"* atau infrastruktur penting dari suatu negara. Infrastruktur penting tersebut meliputi infrastruktur-infrastruktur yang digunakan untuk fasilitas ekonomi, perbankan dan keuangan, transportasi, sistem air, layanan darurat dan teknologi informasi komunikasi dari suatu negara yang apabila terganggu, terdegradasi atau dihancurkan akan menimbulkan dampak yang parah terhadap keamanan, ekonomi, fungsi pemerintahan, kesehatan atau keselamatan masyarakat nasional, atau kombinasi dari hal-hal tersebut.

Penggunaan media yang ditujukan terhadap komponen utama atau sistem dari infrastruktur penting suatu negara tersebut apabila menimbulkan suatu dampak yang parah terhadap penduduk maupun objek sipil, meskipun tidak merusak atau menyebabkan cedera dan kematian dapat digolongkan sebagai serangan bersenjata apabila dampak yang dihasilkan berakibat setara atau menyebabkan cedera atau kematian pada orang atau kerusakan terhadap benda/objek secara fisik meskipun secara tidak langsung.

Serangan-serangan siber yang dilancarkan oleh Rusia beberapa di antaranya telah menargetkan dan menyebabkan terhambatnya kinerja *critical infrastructures* yang dimiliki oleh Georgia, sehingga menyebabkan terhambatnya kemampuan militer dan masyarakat Georgia dalam hal mendapatkan informasi dan komunikasi. Serangan siber Rusia juga menyebabkan banyaknya propaganda dan manipulasi terhadap opini-opini yang ada dalam masyarakat Georgia maupun Internasional. Meskipun serangan siber tersebut memiliki dampak yang cukup signifikan terhadap konflik yang secara langsung terjadi, namun belum dapat dikategorikan sebagai serangan bersenjata apabila didasarkan pada *Article 51 UN Charter.* Hal tersebut dikarenakan serangan siber yang dilancarkan oleh Rusia tersebut tidak mencapai dampak yang setara atau mengakibatkan adanya kerusakan bagi objek/benda secara fisik maupun menyebabkan adanya cedera atau kematian terhadap orang, sehingga pemenuhan unsur dalam *self defense* berupa adanya serangan bersenjata tidak terpenuhi.

Kriteria kedua dalam *self defense* adalah adanya kebutuhan *(necessity)* bagi negara untuk melakukan tindakan *self defense.* kriteria *necessity* sebagai hukum kebiasaan internasional secara umum muncul karena adanya keharusan atau kebutuhan bagi negara dalam melakukan serangan balasan sebagai tindakan defensif untuk memukul mundur atau menghentikan serangan bersenjata yang terjadi. Tindakan *self defense* berdasarkan pada kebutuhan tersebut dapat dilakukan oleh suatu negara apabila merupakan satu-satunya cara bagi negara untuk dapat melindungi kepentingan penting dari bahaya yang bersifat parah atau mengancam, sehingga adanya kebutuhan bagi negara untuk melakukan *self defense* tersebut berkaitan erat dengan adanya serangan

bersenjata yang bersifat mengancam. Syarat pertama mengenai adanya serangan bersenjata dalam melancarkan *self defense* bagi Georgia terhadap serangan siber Rusia belum dapat dikatakan terpenuhi, sehingga adanya kebutuhan bagi Georgia untuk dapat melaksanakan haknya untuk membela diri terhadap serangan bersenjata menjadi tidak terpenuhi pula.

Serangan siber Rusia terhadap Georgia di dalamnya memang menyebabkan gangguan atau serangan signifikan yang dilakukan tanpa menimbulkan kerusakan fisik secara langsung terhadap website perusahaan media, komunikasi dan transportasi milik Georgia. Kerusakan tersebut memang dapat berdampak pada sistem target yang berupa manipulasi data atau perusakan data, sehingga dapat berpotensi menyebabkan kerusakan besar atau bahkan hilangnya fungsi dari sistem komputer atau jaringan komputer tersebut. Namun, sebagaimana dijelaskan sebelumnya hal tersebut masih belum dapat dikategorikan sebagai suatu bentuk keharusan bagi Georgia untuk melaksanakan tindakan *self defense* karena tidak terdapat adanya serangan bersenjata maupun serangan yang setara atau berpotensi menyebabkan kerusakan fisik bagi objek/benda bahkan menyebabkan cidera atau korban jiwa.

Kemudian dalam pemenuhan kriteria *necessity,* tindakan Georgia harus merupakan suatu cara untuk melindungi kepentingan penting dari bahaya yang bersifat parah atau mengancam. Serangan siber yang dilancarkan oleh Rusia kebanyakan dilakukan dengan menggunakan media siber yang berupa *site defacement* dan propaganda siber untuk menargetkan situs-situs pemerintahan milik Georgia. Secara umum dalam website tersebut di dalamnya berisikan informasi-informasi mengenai kegiatan kepresidenan atau pemerintahan yang relatif tidak berbahaya. Serangan siber yang dilancarkan oleh Rusia tersebut beberapa di antaranya juga dapat diatasi dalam waktu yang cukup cepat dan tidak berlangsung dalam jangka waktu yang lama, sehingga tidak dapat dianggap sebagai keadaan yang dapat mengancam atau merugikan bagi sistem keamanan negara Georgia.

Berdasarkan pada hal-hal tersebut, maka serangan Georgia menggunakan media siber terhadap beberapa website dan server dari Ossetia Selatan maupun Rusia seperti *OSInform News Agency, OSRadio, dan RIA Novosti* yang dianggap sebagai bentuk *self defense* untuk mencegah lebih banyak serangan diarahkan kepada website dan servernya, tidak dapat dikatakan sebagai suatu kebutuhan *(necessity).* Hal tersebut dikarenakan tidak terdapat adanya serangan bersenjata maupun serangan yang berpotensi akan membahayakan atau menyebabkan ancaman serius terhadap kepentingan nasional negara Georgia.

Kriteria ketiga adalah *proportionality* (kesebandingan) yang mengharuskan serangan yang digunakan oleh Georgia sebagai respon terhadap serangan siber Rusia dilakukan secara wajar untuk mencapai tujuan mempertahankan diri dengan tetap memperhatikan ketentuan-ketentuan dalam Hukum Internasional yang berlaku dalam konflik bersenjata. Serangan siber yang dilakukan oleh Georgia tersebut dapat dianggap sebagai serangan yang tidak proporsional. Pertama, karena serangan siber Georgia tersebut ditujukan kepada Ossetia Selatan. Hal tersebut merupakan serangan yang tidak proporsional dikarenakan Ossetia Selatan selama konflik *cyber warfare* antara Rusia dan Georgia tidak turut serta melancarkan serangan siber pula terhadap Georgia, sehingga adanya serangan yang ditujukan kepada kantor berita, situs-situs dan website dari Ossetia Selatan tersebut dapat tergolong sebagai tindakan yang tidak proporsional dengan serangan yang diterima oleh Georgia.

Serangan siber yang ditujukan oleh Georgia sebagai suatu respons yang dianggap sebagai bentuk pembelaan diri juga tidak ditujukan terhadap *RBN* atau Forum *StopGeorgia.ru.* Namun, serangan tersebut ditujukan terhadap kantor berita dan situs dari *OSInform News Agency, OSRadio, dan RIA Novosti* yang dalam kegiatannya tidak terlibat secara langsung dalam melakukan serangan siber ataupun bekerjasama dengan *RBN* maupun forum *StopGeorgia.ru.* Serangan Georgia tersebut dapat berpotensi untuk memperparah atau memperpanjang konflik antara pihak-pihak yang terkait, sehingga tindakan Georgia yang dimaksudkan untuk mencegah atau menghentikan serangan dapat dikatakan tidak terpenuhi karena dilakukan secara tidak proporsional. Berdasarkan pada hal-hal

tersebut, maka dapat dikatakan bahwa pemenuhan kriteria proporsionalitas sebagai bentuk pembelaan diri bagi Georgia juga tidak terpenuhi.

Serangan siber dapat dikatakan sebagai serangan bersenjata apabila terdapat adanya dampak yang setara dengan penggunaan senjata konvensional, kimia, biologi, maupun nuklir sejalan dengan *Article 51 UN Charter*. Namun, penggunaan media siber dalam cyber warfare meskipun belum dapat dikatakan sebagai serangan bersenjata tetap memiliki dampak yang cukup signifikan, sehingga berpotensi dapat merugikan bagi suatu negara, hal tersebut sebagaimana didasarkan pada *Rule 11 (9) Tallinn Manual 1.0.*

Kesimpulan dan Saran

Berdasarkan uraian dan pembahasan pada bab-bab sebelumnya, maka dapat disimpulkan bahwa penggunaan media siber yang dilakukan oleh Georgia sebagai respons atas serangan siber Rusia tidak dapat dikategorikan sebagai *self defense* berdasarkan pada hukum internasional, dikarenakan:

1. Penggunaan media siber yang dilakukan oleh Georgia tidak sesuai dengan *Article 51 UN Charter* yang mengharuskan adanya serangan bersenjata terlebih dahulu sebelum melakukan self defense. Penggunaan media siber yang dilakukan oleh Rusia terhadap Georgia tidak dapat dikatakan sebagai serangan bersenjata, sehingga tidak memunculkan adanya hak membela diri *(self defense)* bagi Georgia, karena tidak menyebabkan adanya kerusakan fisik bagi objek/benda dan tidak menyebabkan cedera atau kematian baik secara langsung maupun tidak langsung.
2. Penggunaan media siber yang dilakukan oleh Georgia juga tidak dilakukan dengan memenuhi unsur-unsur *self defense* berupa *necessity* dan *proportionality* sebagai syarat-syarat *self defense* sebagaimana tertulis pula dalam *Rule 14 Tallinn Manual 1.0*. Tidak terpenuhinya unsur *necessity* tersebut karena serangan siber Rusia ditujukan terhadap website-website yang di dalamnya berisikan informasi-informasi yang relatif tidak berbahaya dan tidak berlangsung dalam waktu yang lama, sehingga tidak bersifat mengancam hingga memunculkan adanya keharusan *(necessity)* bagi Georgia untuk melakukan tindakan *self defense*. Tidak terpenuhinya unsur *proportionality* dikarenakan serangan siber yang dilancarkan oleh Georgia dilakukan dengan tidak proporsional terhadap situs-situs dan kantor berita milik Ossetia Selatan dan Rusia yang dalam praktiknya tidak bekerja sama maupun turut serta dalam melancarkan serangan siber. Serangan siber Rusia diketahui berasal dari *RBN* dan *StopGeorgia.ru*. Namun, dalam praktiknya serangan siber yang dilancarkan oleh Georgia diarahkan *terhadap OSInform News Agency, OSRadio,* dan *RIA Novosti* yang tidak bekerja sama maupun turut serta dalam melancarkan serangan siber bersama dengan *RBN* maupun *StopGeorgia.ru.*
3. Penggunaan media siber dalam perspektif *cyber warfare* antara Rusia dan Georgia, meskipun tidak dapat dikategorikan sebagai suatu bentuk *self defense*, namun tetap memiliki dampak yang cukup signifikan. Perbuatan Rusia dalam melakukan serangan sibernya tetap memiliki dampak seperti menyebabkan terganggunya infrastruktur-infrastruktur siber tertentu, menghambat kemampuan militer dan masyarakat Georgia dalam hal mendapatkan informasi dan komunikasi, serta dapat mempengaruhi opini-opini publik. Dampak-dampak tersebut, meskipun tidak dapat dianggap sebagai serangan bersenjata, namun berdasarkan pada *Rule 11 (9) Tallinn Manual 1.0* merupakan tindakan yang dapat dianggap sebagai suatu bentuk intervensi terhadap infrastruktur *cyberspace* milik Georgia, sehingga berpotensi dapat merugikan bagi negara Georgia.

Berdasarkan uraian simpulan tersebut maka saran yang dapat dikemukakan adalah: Setiap negara diharapkan menunjukkan komitmennya dengan mengikuti pedoman dan prinsip yang diuraikan dalam *Tallinn Manual*, sebagai sebuah panduan hukum internasional yang berlaku untuk *cyber warfare* meskipun tidak bersifat mengikat. Selain itu, diperlukan adanya suatu aturan hukum tambahan tersendiri yang lebih mengikat untuk menekan dan mengatur ancaman dari *cyber*

warfare. Hal tersebut dikarenakan serangan siber dapat berpengaruh dan berpotensi melanggar batasan-batasan kedaulatan suatu negara mengingat sifat *cyberspace* yang *borderless*, sehingga penting untuk diatur secara lebih jelas dan tegas mengenai hak dan juga kewajiban bagi negara-negara dalam beroperasi di ranah *cyberspace.*

Daftar Referensi

Adolf, H. (1996). *Aspek Aspek Negara dalam Hukum Internasional.* Jakarta: Raja Grafinfo Persada.

Bernard, V. (2016). The Evolution of Warfare. *International Review of the Red Cross*, Vol.97, No. 900.

Bryant, R. (2001). What Kind of Space is Cyberspace ? *Minerva-An Internet Journal of Philosophy 5*, 138-155.

Buchan, R. (2019). *Cyber Espionage and International Law.* UK: Hart Publishing.

Carr, J. (2009). *Inside Cyber warfare.* United States: O'Reilly Media, inc.

Danchev, D. (2008, August 11). *Coordinated Russia vs Georgia cyber attack in progress*. Retrieved from Zdnet: https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/

Green, J. A. (2015). *Cyber warfare: A Multidisciplinary Analysis.* Routledge.

Hollis, D. (2011). Cyberwar Case Study: Georgia 2008. *Small Wars Journal*.

Kiyuna, A., & Conyers, L. (2015). *Cyberwarfare Sourcebook.* Lulu.com.

Kusumaatmadja, M. (2015). *Pengantar hukum internasional.* Jakarta: Binacipta.

Leyden, J. (2008, August 14). *Bear prints found on Georgian cyber-attacks*. Retrieved from The Register: https://www.theregister.com/2008/08/14/russia_georgia_cyberwar_latest/

Markoff, J. (2008, August 12). *Before the Gunfire, Cyberattacks*. Retrieved from The New York Times: https://www.nytimes.com/2008/08/13/technology/13cyber.html

Melzer, N. (2011). *Cyberwarfare and International Law.* United Nations Institute for Disarmament Research.

Melzer, N. (2016). *International humanitarian law: A comprehensive introduction.* International Committee of the Red Cross.

Murray, A. D. (2007). *The Regulation of Cyberspace: Control in the Online Environment.* London: Routledge-Cavendish.

Nugraha, P. C. (2013). Konsepsi Kedaulatan Negara dalam Borderless Space. *Opinio Juris: Jurnal Hukum dan Perjanjian Internasional*.

Sari, I. Y. (2020). *Keamanan Data dan Informasi .* Kisaran: Yayasan Kita Menulis.

Schmitt, M. (2012). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framewok. *Colombia Journal of Transnational Law*, 379-431.

Simorangkir, J., Erwin, R., & J.T, P. (2013). *Kamus Hukum.* Bintan: Sinar Grafika.

Sjahdeini, S. R. (2009). *Kejahatan & TIndak Pidana Komputer.* Jakarta: Pustaka Utama Grafiti.

Tampubolon, K. E. (2019). Perbedaan Cyber Attack, Cybercrime, dan *Cyber warfare*. *Jurist-Diction: Vol. 2 No. 2*.

Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations.* Tallinn: Cooperative Cyber Defence Centre of Excellence (CCD COE).

Tskhinvali. (2008, August 5). *S.Ossetian News Sites Hacked*. Retrieved from Civil.ge: https://civil.ge/archives/116892

Udoji, A., & Cappello, D. (2008, August 11). *The digital frontline in the Georgia conflict*. Retrieved from TheWorld: https://theworld.org/stories/2008-08-11/digital-frontlines-georgia-conflict

Ventre, D. (2012). *Cyberwar and Information Warfare.* John Wiley & Sons.

Warren, P. (2007, November 15). *Hunt for Russia's web criminals*. Retrieved from The Guardian: https://www.theguardian.com/technology/2007/nov/15/news.crime