ANALISIS YURIDIS MENGENAI CYBER ATTACK DALAM CYBER WARFARE BERDASARKAN HUKUM HUMANITER INTERNASIONAL

(Studi Kasus Cyber attack Negara Amerika Serikat Terhadap Program Pengembangan Nuklir Negara Iran Pada Tahun 2009)

ARTIKEL ILMIAH

Diajukan Untuk Memenuhi Sebagian Syarat- Syarat Memperoleh
Gelar Kesarjanaan Dalam Ilmu Hukum

Oleh :
MIKO ADITIYA SUHARTO
NIM. 0910110191

KEMENTERIAN RISET TEKNOLOGI DAN PENDIDIKAN TINGGI
UNIVERSITAS BRAWIJAYA
FAKULTAS HUKUM
MALANG
2015

Analisis Yuridis Mengenai *Cyber-Attack* Dalam *Cyber Warfare* Berdasarkan Hukum Humaniter Internasional

(Studi Kasus *Cyber-Attack* Negara Amerika Serikat Terhadap Program Pengembangan Nuklir Negara Iran Pada Tahun 2009)

Miko Aditiya Suharto, Sucipto, S.H., M.H., Herman Suryokumoro, S.H., M.S.

Fakutas Hukum Universitas Brawijaya

Email : *Micko.alzalel04@yahoo.co.id*

ABSTRAK

Program nuklir Iran terhenti, virus komputer canggih menyerang, sentrifugal reaktor nuklir berputar tak terkendali. A *"distributed denial of service"* serangan menyabotase seluruh komputer penduduk Burma secara offline sebelum pemilu nasional pertama di negara itu dalam dua puluh tahun. Militer China menyerang situs web Falun Gong yang berbasis di Alabama. Apa hukum mengatur "serangan cyber" ini? Apakah hukum perang berlaku? Jika tidak, apa yang badan-badan lain hukum dapat membantu mengatasi masalah? Pasal ini membahas pertanyaan-pertanyaan ini dan, dalam proses, menawarkan wawasan baru bagaimana hukum yang ada dapat diterapkan dan disesuaikan dan diubah untuk memenuhi tantangan yang ditimbulkan oleh serangan cyber. Artikel ini meneliti tentang pertanyaan-pertanyaan di atas melalui analisis terhadap kasus serangan cyber Amerika Serikat terhadap Program nuklir Iran. Penelitian dari kasus ini dilakukan dengan mencari konsep dari cyber-attack melalui definisi serangan konvensional lalu dianalisa dengan Instrumen-instrumen hukum yang ada. Dengan demikian dapat diuraikan unsur-unsur yang dapat menjadi kunci dalam memberikan solusi hukum terhadap ancaman yang muncul dari serangan cyber di masa yang akan datang.

Kata Kunci : Cyber-attack, Stuxnet, Cyber Warfare, Amerika Serikat, Iran.

ABSTRACT

Iran's nuclear program grind to a halt, a sophisticated computer virus attack, nuclear reactor centrifugal spinning out of control. A "distributed denial of service" attack takes the entire population of Burma offline immediately before the country's first national election in twenty years. China's military mounts an attack on a Falun Gong Website based in Alabama. What law regulates these "cyber-attacks"? Does the law of war apply? If not, what other bodies of law might help address the problem? This article discusses these questions and, in the process, offering new

insights into how existing laws can be applied and adapted and modified to meet the challenges posed by cyber attacks. This article examines the above questions through an analysis of the case of the US cyber attack against Iran's nuclear program. The study of this case is done by finding the concept of cyber-attack through the definition of a conventional attack and then analyzed by instruments of existing law. Thus it can describing the elements that can be the key in providing legal solutions to the emerging threat of cyber attacks in the future.

Keywords : Cyber-attack, Stuxnet, Cyber Warfare, USA, Iran.

PENDAHULUAN

Latar Belakang

Cyber space atau di dalam bahasa Indonesia disebut sebagai dunia maya yaitu, sebuah domain operasional yang menggunakan elektro dan elektromagnetik, untuk membuat, menyimpan, memodifikasi, serta saling menukar informasi.[1] Internet bisa digunakan siapa saja entah individu, badan usaha, bahkan Negara sekalipun. Dalam hal kenegaraan Internet berfungsi sebagai salah satu sarana untuk melakukan hubungan dengan Negara satu dengan Negara lainnya salah satu contohnya adalah Internet digunakan sebagai sarana untuk melakukan hubungan Diplomatik secara jarak jauh. Tidak hanya digunakan untuk sarana melakukan hubungan Diplomatik saja, Baru-baru ini dapat dijumpai teknologi Internet digunakan oleh Negara-negara yang bersengketa sebagai jalan lain untuk melancarkan serangan terhadap Negara lawannya secara tidak langsung. Sebagai salah satu contoh adalah *Cyber-attack* Amerika terhadap Reaktor pembangkit listrik tenaga nuklir milik negara Iran yang menjadi pokok bahasan pada penelitian ini. *Cyber-attack* yang dilakukan Amerika Serikat di latar belakangi oleh hal-hal bersifat politik, dan ada suatu unsur perintah yang resmi dari pemerintah suatu negara dengan kata lain melegalkan dan mendukung serta memfasilitasi Pada Juni 2009 terdeteksi sebuah virus dalam sistem komputer Pembangkit listrik tenaga nuklir di Natanz, Iran. Di ketahui serangan ini

[1]Kuehl, Dan, From *Cyber space* to Cyberpower: Defining the Problem, Information Operations at the National Defense University, USA, www.carlisle.army.mil/DIME/documents/ (20 Februari 2013)

adalah *Preemptive military strike*[2] yang dilakukan oleh Amerika Serikat. Hal tersebut diketahui berdasarkan Presiden Amerika Serikat Barack Obama yang dalam pernyataannya memutuskan untuk mempercepat serangan yang dimulai sejak pemerintahan Presiden George W. Bush pada tahun 2006 dengan kode bernama Olimpic-games dalam pertemuan di gedung putih. File virus ini lolos dan merambat ke komputer di seluruh dunia pada musim panas 2010 melalui Internet setelah terjadi ketidaksengajaan dalam pemrograman,[3] Pakar keamanan komputer yang telah dikembangkan oleh Amerika Serikat dan Israel mulai mempelajari virus worm tersebut memberinya nama Stuxnet.[4] Stuxnet mampu menyusup masuk dan menyabot sistem dengan cara memperlambat ataupun mempercepat motor penggerak Reaktor Nuklir, bahkan dapat membuatnya berputar jauh di atas kecepatan maksimum. Kecepatan ini akan menghancurkan sentrifuse atau setidaknya merusak kemampuan komponen reaktor untuk memproduksi bahan bakar uranium.

Dalam pertemuan di gedung putih yang membahas tentang lolosnya virus komputer jenis worm ini, Pertimbangan Presiden Barrack Obama, wakil presiden Joseph R. Biden Jr, dan Mantan Direktur CIA Leon Panetta dalam upaya memperlambat kemajuan perkembangan program nuklir Iran telah gagal dikompromikan, sehingga Presiden Obama ingin segera mempercepat upaya dalam melumpuhkan perkembangan teknologi nuklir di Iran dengan mengirimkan serangan *malware*[5] berikutnya. Ini menjadi pertama kalinya bagi Amerika Serikat menggunakan *Cyber Weapon* secara berkali-kali dalam melumpuhkan infrastruktur lawannya, yang mana biasanya yang dilakukan oleh Amerika adalah mengirimkan Agen untuk espionase atau langsung mengebom Negara lawan.

Menurut *Tallin Manual* yang sekarang telah disahkan dan berlaku mulai maret 2013 lalu oleh NATO *cyber defense* di Estonia, *Cyber-attack* Amerika ke Iran

---

[2]Aksi militer terhadap bangsa yang lain untuk mencegah atau mengurangi serangan militer diduga dari bangsa lain yang diwaspadainya.

[3]Sanger , David. E., 2012, Obama Order Sped Up Wave of *Cyber attack*s Against Iran, The New York Times: Middle East, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-*Cyber attack*s-against iran.html?_r=2& diakses 25 maret 2013

[4]*Ibid*

[5]*Malware* atau *Malicious software* memiliki pengertian piranti lunak atau aplikasi data yang memiliki sifat merusak

merupakan bentuk *"Use of Force"*. Menurut *The Tallinn Manual on the International Law Applicable to Cyber warfare Rule 11:*[6] *"'Use of Force' is 'Acts that kill or injure persons or destroy or damage objects are unambiguously uses of force.'"*

Sesuai *United Nation Charter*, penggunaan kekuatan (Kekerasan) dilarang, kecuali dalam membela diri." Dengan adanya *Use of Force* yang dilakukan Amerika, bisa dikatakan hal tersebut sebagai *Hostility act* Negara Amerika terhadap Iran yang dapat dikatakan sebagai tanda awal mula konflik seperti yang dinyatakan dalam hukum humaniter Internasional dalam Konvensi Jenewa 1949.

Sedangkan Virus *Stuxnet* yang digunakan dalam *Cyber-attack* di dalam penerapannya di dalam suatu konflik bersenjata, dapat dikatakan sebagai senjata yang digunakan dalam penyerangan di dalam *Cyber-attack* Amerika Serikat dalam Pengaturannya dalam *Tallinn Manual Rule 41* menyatakan :[7] *"Cyber Weapons are cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as an attack."*

Pengertian dari *Cyber Weapon* ini masih belum cukup luas dan masih sulit untuk diterapkan dalam praktiknya sehingga menimbulkan celah hukum yang dapat dijadikan alasan negara-negara berkepentingan dalam melakukan pelanggaran hukum.

Dalam menanggapi serangan ini belum ada serangan balasan dari pihak Negara Iran. Apabila Iran melakukan *Cyber-attack* balasan terhadap *Cyber-attack* Amerika Serikat maka dapat dikatakan sebagai perang (*Cyber warfare*). Jika memang dapat dikategorikan sebagai perang maka medan perang bukan hanya di darat, laut, udara, dan ruang angkasa saja tetapi di dunia maya (*Cyber space*) juga.

---

[6] *Talinn Manual on the International Law Applicable to Cyber warfare Rule 11*
[7] *Talinn Manual on the International Law Applicable to Cyber warfare Rule 41*

Rumusan Masalah

Berdasarkan latar belakang masalah yang ada, maka penulis dapat merumuskan pokok permasalahan dari penelitian ini adalah sebagai berikut:

1. Bagaimanakah status hukum tindakan *Cyber-attack* Amerika Serikat terhadap pembangkit tenaga Nuklir Iran dapat dikategorikan sebagai Pelanggaran Yuridiksi Negara apabila ditinjau berdasarkan Hukum Humaniter Internasional?
2. Apakah Virus *Stuxnet* yang digunakan dalam *Cyber-attack* oleh Amerika Serikat terhadap pembangkit tenaga Nuklir milik Iran dapat dikategorikan sebagai senjata apabila ditinjau dari Hukum Humaniter Internasional yang berlaku?

PEMBAHASAN

Metode Penelitian

Jenis penelitian ini adalah penelitian yuridis normatif yaitu penelitian terhadap permasalahan-permasalahan hukum yang menjadi obyek kajian, dianalisis berdasarkan pada sumber-sumber hukum berupa peraturan-peraturan hukum yang berlaku, teori-teori hukum dan doktrin-doktrin para sarjana hukum terkemuka.. Pendekatan penelitian yang digunakan dalam karya ilmiah ini yaitu pendekatan perundang-undangan (*statute approach),* pendekatan konsep *(conceptual approach),* dan pendekatan kasus atau *case approach.*

Hasil Penelitian

A. *Analisis Cyber-attack* Amerika Serikat terhadap Iran Menurut Hukum Humaniter Internasional

Tujuan dibuatnya *Tallinn Manual On International Law Applicable At Cyber Warfare* adalah untuk memenuhi kebutuhan hukum dalam mengatur peperangan yang terjadi di *cyberspace.* Dengan mengacu pada *Jus ad bellum* dan *Jus in Bello* dalam hukum humaniter internasional, Tallinn Manual selain mengatur peperangan dari sudut hukum perang, Tallinn Manual juga mengatur tentang peperangan dari sudut hukum hak asasi manusia juga.

Dalam praktiknya serangan dihubungkan dengan kehancuran *(destroy)* atau kerusakan *(damage)*, dalam hal ini belum ada definisi yang formal mengenai kehancuran maupun kerusakan di dalam hukum humaniter internasional.[8] Di dalam suatu pertempuran atau peperangan, hancurnya suatu benda pasti karena adanya suatu serangan, namun hal tersebut banyak diragukan karena, serangan tidak selalu identik dengan kehancuran, contohnya ketika Amerika menginvasi Irak, serangan pasukan udara Amerika dengan menembakkan gelombang eletromagnetik (EMP) ke jaringan satelit televisi milik Irak untuk melumpuhkan semua perlengkapan dan peralatan penyiaran.[9] Beberapa ahli sependapat bahwa serangan *(attack)* bila di hadapkan dengan hukum humaniter menjadi serangan bersenjata *(armed attack)*, menurut Jean Pictet, serangan bersenjata terkait dengan durasi dan intesitas yang memadai. Namun, tidak sedikit ahli yang menanggapi bahwa, durasi dan intensitas sebagai patokan terhadap suatu serangan dirasa masih belum cukup, Michael N. Schimitt mengemukakan 6 kriteria untuk dapat memenuhi sebagai suatu serangan;[10]

1. ***Severity***, dilihat dari ruang lingkup dan intesitas serangan tersebut, seperti banyaknya korban jiwa yang diakibatkan, luas area yang terkena dampaknya dan banyaknya benda-benda yang rusak karena serangan tersebut
2. ***Immediacy***, melihat pada durasi dari serangan tersebut, seperti berapa banyak waktu yang dibutuhkan agar efek dari serangan tersebut dapat dirasakan, dan berapa lama efek dari serangan tersebut terjadi,
3. ***Directness***, melihat pada luka atau kerusakan yang di timbulkan oleh adanya serangan tersebut,
4. ***Invasiveness***, melihat pada locus dari serangan tersebut, maksudnya bagaimana serangan tersebut melintasi batas-batas Negara,
5. ***Measurability***, yaitu akibat dari serangan tersebut dengan melakukan penafsiran dan pengukuran,

---

[8]Hayashi, Nobuo, 2010, *Requirement of Military Necessity in International Humanitarian Law and International Criminal Law, Boston University Internasional Law Journal*, hal. 110
[9]*Ibid* hal. 111
[10]Carr, Jeffrey, 2010, *Inside Cyber Warfare*, O'Reilly, hal. 60

6. ***Presumptive Legitimacy***, melihat pada penilaian serta legitimasi dari serangan tersebut yang didasarkan pada praktik Negara-Negara, dan norma-norma yang ada di dalam komunitas internasional, suatu tindakan dapat memperoleh legitimasi berdasarkan hukum ketika hal tersebut diterima oleh komunitas internasional.

Memanfaatkan kondisi perang dingin yang terjadi, dan dengan alasan Program senjata nuklir Iran menjadi ancaman Keamanan nasional Israel dan akan memicunya semakin berkembangnya tindakan terorisme dari organisasi militan, Israel dan Amerika Serikat memilih untuk melakukan tindakan pencegahan pertama yang merupakan kebijakan luar negeri dalam strategi keamanan nasional Amerika Serikat yaitu *Pre-emptive Military Strike.*

Doktrin mengenai *pre-emptive military strike* diusulkan oleh Presiden Amerika Serikat *George W. Bush* dalam pidatonya di *West Point* pada 1 Juni 2002.[11] Menurut Presiden *George W. Bush Pre-emptive military strike* adalah strategi keamanan nasional Negara Amerika Serikat dengan mempersiapkan penggunaan *pre-emptive military force* yang ditujukan kepada suatu negara tertentu untuk pencegahan terhadap pihak musuh agar tidak menggunakan senjata pemusnah masal/*weapon of mass destruction (WMD)* terhadap Negara Amerika atau terhadap Negara sahabat maupun sekutu dari Negara Amerika.[12]

Bentuk dari *pre-emptive military strike* dilakukan oleh Amerika Serikat terhadap Negara Iran adalah mengirimkan *malware* berupa *computer virus* jenis *worm* yang kemudian virus komputer ini diberi nama *Stuxnet. Stuxnet* mampu menyusup masuk dan menyabot sistem dengan cara memperlambat ataupun mempercepat motor penggerak Reaktor Nuklir, bahkan dapat membuatnya berputar jauh di atas kecepatan maksimum. Kecepatan ini akan menghancurkan sentrifuse atau

---

11See speeches of President George W. Bush at West Point on June 1, 2002 at [http://www.whitehouse.gov/news/releases/2002/06/20020601-3.html]; and the UN on September12, 2002 at [http://www.whitehouse.gov/news/releases/2002/09/20020912-1.html]; WashingtonPost, June 2, 2002, p. A1; Washington Post, September 13, 2002, p.A1. The National Security Strategy of the United States of America is found at [http://www.whitehouse.gov/nsc/nss.html].

12Grimmett F. Richard , 2003, U.S. Use of preemptive Military Force, CRS Report for congress, www.fas.org/man/crs/RS21311.pdf *diakses pada 12 Maret 2014*

setidaknya merusak kemampuan komponen reaktor untuk memproduksi bahan bakar uranium.

Doktrin *pre-emptive military strike* ini sendiri dalam penerapannya tidak selaras dengan prinsip-prinsip umum yang diakui dalam hukum internasional, terutama prinsip *non-use act of force* dan *non-Intervention.* Dalam *Tallinn Manual on International Law applicable to cyber warfare* sendiri mengatur mengenai *Use of Force*, hal tersebut tercantum pada *Chapter II*, *The Use Of Force*, *Section I : Prohibition of the use of Force* pada *Rules 10-12* yang mengacu pada *United Nation Charter, Chapter I: Purposes And Principles. United Nation Charter Article 2 (4).*

Cyber-attack yang dilakukan oleh Amerika Serikat dan Israel termasuk dalam kategori *cyber operation* dan sesuai dengan ketentuan di atas telah melanggar ketentuan mengenai larangan penggunaan kekerasan di dalam teritorial negara Iran. Teritorial negara Iran yang dimaksud dalam hal ini adalah Wilayah *cyberspace* yang berada dalam Yurisdiksi negara Iran. Di dalam Yurisdiksinya, Negara Iran berhak dan berdaulat penuh untuk menentukan nasibnya sendiri tanpa adanya intervensi dari negara lain.

Dari pernyataan di atas Negara Iran secara bebas sesuai dengan hak kedaulatannya untuk mengatur setiap *cyber infrastructure* dan *cyber activities* yang ada di wilayah negaranya sesuai dengan Tallinn Manual *Rule 1 Commentary 5*.[13] Commentary 5 menyatakan Kedaulatan yang dimiliki oleh suatu Negara di dalam teritorialnya terhadap *cyber infrastructure,* yang pertama, *cyber infrastructure* tersebut merupakan benda yang tidak dilarang secara hukum oleh negara tersebut. Kedua, Kedaulatan dari negara untuk melindungi *cyber infrastructure,* tidak masalah *cyber infrastructure* tersebut milik pemerintah, kelompok tertentu, ataupun milik individu. Selanjutnya dalam *Commentary 6*, menjelaskan *cyber operation* yang dilakukan oleh suatu negara terhadap *cyber infrastructure* negara lain, dianggap sebagai pelanggaran terhadap Kedaulatan. Penyerangan yang dilakukan oleh Amerika Serikat dan Israel terhadap infrastruktur nuklir Iran jelas telah melanggar kedaulatan

13 *Tallinn Manual on International law applicable at cyber warfare, rule 1, commentary 5*

Negara Iran dalam mengatur urusan dalam negerinya sendiri tanpa campur tangan dari bangsa lain.

Alasan Amerika Serikat dan Israel dalam melakukan *Cyber-attack* sebagai perwujudan dari Doktrin *Preemptive military strike* sebagai tindakan pencegahan dengan maksud melakukan perlindungan diri dari potensi ancaman Negara Iran mengembangkan teknologi nuklir untuk membuat senjata, tidak dapat dibenarkan karena tidak adanya serangan bersenjata dari pihak Iran. Ketentuan dalam *United Nation Charter, Chapter VII: Action With Respect To Threats To The Peace, Breaches Of The Peace, And Acts Of Aggression Article 51 yang* dijadikan acuan dari *Tallinn Manual on International Law applicable to cyber warfare, Section 2 ; self Defence Rules 13-17* membuat alasan Amerika Serikat melakukan *Cyber-attack* sebagai perwujudan dari Doktrin *Preemptive military strike* untuk melakukan tindakan pencegahan dengan maksud melakukan perlindungan diri dari potensi ancaman Negara Iran mengembangkan teknologi nuklir untuk membuat senjata, tidak dapat dibenarkan karena tidak adanya serangan bersenjata dari pihak Iran sehingga unsur *if an armed attack occurs* dalam *United Nations Charter article 51* tidak terpenuhi, sehingga alasan dari Amerika Serikat dan Israel terhadap mengirimkan virus stuxnet tersebut dapat dikatakan tidak sah.

Dari analisis di atas tindakan dari Amerika Serikat dan Israel dalam melakukan *Cyber-attack* justru memenuhi unsur-unsur dari tindakan Agresi terhadap bangsa lain yang ada pada Resolusi Majelis Umum Nomor 3314 (XXIX) artikel 1.

B. Virus Stuxnet Sebagai Senjata Dalam Konflik Kekerasan Bersenjata Berdasarkan Hukum Humaniter Internasional

1. *Cyber Weapon* Sebagai Sarana dan Metode Berperang Dalam *Cyber Warfare*

Dalam berperang Kombatan mempunyai hak untuk memilih sarana dan metode berperangnya sendiri yang diatur dan dibatasi oleh hukum humaniter internasional, adapun pengaturan dan pembatasan tersebut dapat ditemukan dalam *Additional Protocol I in 1977 mengenai the Protection of Victims of Interntional Armed Conflict*. Selain itu terdapat juga peraturan tentang pelarangan penggunaan

senjata seperti senjata biologi, senjata yang mempunyai efek membakar, senjata yang membutakan, dan ranjau.[14]

Article 36 Additional Protocol I of Geneva Convention, relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1977 bertujuan untuk mencegah penggunaan senjata-senjata baru, sarana dan metode berperang baru yang mempunyai efek-efek yang secara umum dilarang di dalam hukum internasional. *Article 36* diatas juga di lengkapi dengan adanya *Article 82 Additional Protocol I*, di mana artikel tersebut banyak dibutuhkan oleh para penasihat hukum atau ahli hukum untuk melakukan pembelaan terhadap *military commanders* atau komandan militer.[15]

Dengan memanfaatkan celah hukum dari peraturan yang ada dalam hukum perang, semakin banyak negara-negara yang memanfaatkan *cyberspace* sebagai matra dalam melakukan *cyber warfare*, Ketentuan-ketentuan yang telah ada dalam hukum humaniter Internasional menjadi tidak sesuai atau bahkan tidak berlaku dikarenakan unsur-unsur perbuatan dalam peraturan yang mengatur tentang perang dan senjata yang digunakan tidak terpenuhi.

Menurut Stefano Mele, Memisahkan antara *cyber-crime* dan *cyber-espionage* sangatlah penting di dalam membangun konsep definisi dari *cyber weapon*, yang menjadi alasan utama dalam hal ini adalah penggunaan dari sebuah *cyber weapon* dapat memicu terjadinya konflik sebuah negara.[16] Berdasarkan pertimbangan ini dapat dikatakan bahwa senjata juga bisa memiliki bentuk yang abstrak tidak harus memiliki wujud konkrit. Melalui pertimbangan ini, suatu kesatuan instruksi/perintah komputer, salah satu contohnya adalah sebuah program komputer, kode yang merupakan sebagian dari sebuah program, dan lain-lainnya, dapat disebut sebagai sebuah senjata, ketika digunakan pada konteks tertentu dalam hal ini sebagai alat untuk melakukan serangan dengan maksud menyabotase atau merusak/melukai obyek

---

[14]*Anonymous, 2006, **A Guide to The Legal Review of New Weapon**, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol 1 of 1977, International Committee of The Red Cross,* www.icrc.org/eng/assets/files/other/irrc_ 864_icrc_ geneva.pdf, hal. 932

[15]Anonymous, 2006, Op.cit, hal. 933

[16]Stefano Mele, 2013-2014, *Op.Cit* Hal. 57

atau subyek yang telah ditentukan, melalui suatu alat. Suatu alat yang dimaksudkan adalah perangkat komputer dan jaringan Internet.[17] Stefano Mele juga menyatakan untuk mencapai definisi tersebut, perlu untuk difokuskan pada tiga elemen mendasar, yaitu :[18]

1. ***CONTEXT****: it must be typical context of an act of cyber warfare. This concept may be defined as a conflict among actors, both National and non-National, characterized by the use of information system, with purpose of achieving, keeping, or defending acondition of strategic, operative and/or tactical advantage.*
2. ***PURPOSE****: of causing, even inderictly, physical damage to object or people; or of sabotaging and/or damaging in a direct way the information systems of a sensitive target of the attacked subject.*
3. ***MEAN/TOOL****: an attack performed through the use of information system, including the internet.*

Dari ketiga unsur di atas, Stefano Mele menarik kesimpulan dan mendefinisikan bahwa *cyber weapon* adalah :

"A part of equipment, a device, or any set of computer instructions, used in a conflict among actors both National and non-National, with the purpose of causing (directly or otherwise) physical damage to objects or people, or of sabotaging and/or damaging in a direct way the information systems of a sensitive target of the attacked subject."

Menurut Tallinn Manual on International Law Applicable at Cyber Warfare Rule 41 - *Definitions of Means and Methods of Warfare, Commentary 2 :*

For the purposes of this Manual, cyber weapons are cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as an attack (Rule 30). The term means of cyber warfare encompasses both cyber weapons and cyber weapon systems. A weapon is generally understood as that aspect of the

[17] *Ibid*
[18] *Ibid*

system used to cause damage or destruction to objects or injury or death to persons. Cyber means of warfare therefore include any cyber device, materiel, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber attack (Rule 30).

Dari pendapat di atas dapat disimpulkan, bahwa terdapat senjata baru yang lahir dari pemanfaatan teknologi computer beserta sistem informasinya yang dapat digunakan sebagai salah satu metode dalam berperang yaitu *Cyber weapon*.

2. Metode-Metode *Cyber-attack* Dalam *Cyber Warfare*

Terdapat banyak jenis *cyber weapon* dan cara untuk melakukan penyerangan *(cyberattack)* terhadap sistem komputer namun di sini hanya akan di paparkan beberapa cara atau media umum yang digunakan dalam *Cyber warfare* yaitu :[19]

1) *Malware (Malicious Software)*

Terdapat beberapa jenis *malware* yang umum dikenal dan sering menyerang sistem komputer seperti *Virus, Worm, Trojan Horse, Backdoors, Keystroke Logger, rootkit atau Spyware.*

2) DoS (Denial of Service)

Denial of Service adalah aktifitas yang bertujuan untuk menghambat kerja sebuah layanan (service) atau mematikannya, sehingga user yang berhak atau yang berkepentingan tidak dapat menggunakan layanan tersebut, serangan DoS mentargetkan bandwidth dan koneksi sebuah jaringan untuk dapat mencapai misinya.[20] Pada serangan terhadap bandwidth, sang penyerang melakukan pembanjiran lalulintas data dalam suatu jaringan, dengan menggunakan perangkat yang sudah tersedia pada jaringan itu sendiri, sehingga membuat user yang sudah terkoneksi di dalam nya mengalami hilang koneksi.

3) *BotNet*

Terdapat banyak istilah-istilah yang memaparkan apa itu *bot* atau *botnet.* Menurut John Tay dan Jeffrey Tosco pada presentasinya di *APNIC Training,*[21]

---

[19]Chad Nelson, ***Cyberwarfare: The Newest Battlefield***, Washington University in St. Louis, http://www.cse.wustl.edu/~jain/cse571-11/ftp /cyberwar.pdf diakses 12 Oktober 2013

[20]*Ibid*

[21]*Ibid*

menyatakan bahwa *bot* merupakan software yang bekerja secara otomatis (seperti robot) dalam menyebarkan dirinya ke sebuah host secara diam-diam dan menunggu perintah dari *botmaster*. *botnets* sudah menjadi suatu bagian penting dari keamanan jaringan internet, karena sifatnya yang tersembunyi pada jaringan *server* internet.

3. Metode-Metode Cyber Defense Dalam Cyber Warfare

Dalam strategi berperang selain menyerang juga ada strategi bertahan. Begitu juga di dalam *cyber warfare*, bila tindakan *offensive* di dalam *Cyber warfare* disebut dengan *cyber-attack*, untuk menangkal tindakan *offensive* tersebut diperlukan suatu metode *Defensive* yang memanfaatkan teknologi komputer juga. Terdapat beberapa metode dalam bertahan antara lain yaitu;

a) *Active Defense*

Active defense adalah serangkaian tindakan yang bertujuan untuk melakukan tindakan preventif dan dapat juga melakukan tindakan balasan atau retaliasi dari *cyber threat*, salah satu bentuk dari pertahanan ini yang sering digunakan adalah metode *Honeypot.* Cara kerja dari metode Honeypot ini, membuat jaringan palsu *(fake network)* yang dilekatkan atau dipasangkan pada jaringan yang telah diproteksi, dan secara sengaja membiarkan beberapa lubang atau celah keamanan tetap terbuka dan aman.[22] Celah tersebut apabila dianalogikan berfungsi layaknya perangkap yang telah diberi umpan. Dengan menggunakan metode Honeypot ini seorang administrator dapat menemukan atau melacak siapa yang telah menyerang dan memasuki sistem keamanan komputernya.

b) *Passive Defense*

Passive Defense merupakan serangkaian tindakan yang bertujuan untuk melindungi sistem komputer dari *cyber threat*, dengan memberdayakan program seperti :

[22]Eric, Peter, *A Practical Guide to Honeypot*, Washington University in St. Louis, http://www.cse. wustl.edu /~jain/cse571-09/ftp/honey/index.html#sec1.2 (1 Desember 2014)

1) *Firewall*

   Program *Firewall* bekerja dengan cara melakukan monitoring terhadap cyber threat yang memiliki potensi membahayakan sistem komputer melalui koneksi yang masuk. *Firewall* selanjutnya akan melakukan penolakan terhadap threat tersebut.

2) *Antivirus*

   Piranti lunak (software) Antivirus bekerja dengan cara melakukan pemindaian terhadap file-file yang ada di dalam komputer maupun yang akan masuk ke dalam komputer untuk memastikan file-file tersebut aman dan tidak membahayakan sistem komputer.[23]

3) *Access Control*

   Metode *Access Control* adalah metode pemberian izin *(permission)* yang berbeda kepada setiap pengguna dan komputer dalam melakukan akses. Tujuan metode ini adalah untuk mencegah komputer atau akun pengguna yang telah mengalami gangguan atau mengandung *threat* merusak dan menginfeksi seluruh sistem jaringan yang ada. Kebanyakan perusahaan masing-masing memiliki metode *Access control* yang berbeda-beda diterapkan di komputer atau sistem jaringannya.[24]

4. Analisis Virus Stuxnet Amerika Serikat sebagai *Cyber Weapon*

Setelah Tallinn Manual disahkan dan didistribusikan melalui *Cambridge University* pada tahun 2013 lalu, Tallin Manual menjadi salah satu sumber hukum dalam memenuhi kebutuhan hukum masyarakat Internasional mengenai persoalan *cyber warfare*. Keterangan mengenai *Cyber Weapon*, pada Tallinn Manual *On International Law Applicable To Cyber Warfare* dinyatakan dalam *Rule* 41 *Definition of means and Methods of Warfare*, *Commentary 2.* Ketiga unsur yang dinyatakan oleh Stefano Mele, yaitu *Context, Purpose,* dan *Mean/Tool* mengenai *cyber weapon* dalam hal ini terletak pada poin-poin *Rule* 41 (b). Mengenai ***Context***

[23]*Nelson, Chad, Loc.cit*
[24]*Ibid*

dari *cyber weapon* ada pada Tallinn Manual, *Rule* 41, *Commentary* 1.

Dari *Rule* 41 *Commentary* 1 yang menyatakan sebagai Context adalah *cyber operation,* yang dimana cyber operation memiliki konteks penggunaan atau pemanfaatan dari sistem informasi dan kalimat *this Rule are applicable in both international and non-international armed conflict* menjelaskan para pihak yang melakukan konflik dalam skala Internasional maupun non-Internasional. Unsur kedua ***Purpose*** ada pada Tallinn Manual, *Rule* 41, *Commentary* 2. Kalimat "*For the purposes of this Manual, cyber weapons are cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as an attack"* menjelaskan niat dan tujuan dari para pihak dalam menggunakan teknologi sistem informasi dan komputer untuk menyebabkan kerusakan pada obyek atau luka pada seseorang secara langsung maupun secara tidak langsung. Unsur yang ketiga yaitu ***Mean/Tool*** juga ada pada Tallinn Manual, *Rule* 41, *Commentary 2* terletak pada kalimat : *Cyber means of warfare therefore include any cyber device, materiel, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber attack.* Sehingga dapat disimpulkan istilah dari *cyber weapon* yang ada pada *Tallinn Manual on International Law Applicable To cyber warfare* telah memenuhi ketiga unsur dari *cyber weapon* dan dapat digunakan sebagai penutup celah hukum mengenai penggunaan *cyber weapon* yang sebelumnya tidak ada.

Dari penjelasan dasar di atas, Stuxnet dapat diklasifikasikan sebagai *cyber weapon*. Hal tersebut tampak pada pertama, dalam *CONTEXT*, virus stuxnet merupakan perintah komputer dalam bentuk program *(malware)* yang dapat dijalankan dan digunakan oleh Negara Amerika Serikat dalam melakukan *cyber-attack* terhadap pembangkit nuklir Iran. Hal tersebut menunjukan para pihak yang menjadi aktor dari konflik tersebut adalah Amerika Serikat dan Iran. Fakta di atas sesuai dengan Tallinn Manual, *Rule* 41, *Commentary* 1.

Kedua, dalam memenuhi unsur *PURPOSE*, kode perintah yang digunakan dalam menyusun virus stuxnet dimodifikasi sedemikian rupa, sehingga saat

dijalankan secara langsung hanya memberikan *cyber-threat* dalam bentuk menyabotase dan merusak sistem informasi tertentu milik target yang dalam kasus ini adalah sistem komputer dan reaktor nuklir yang ada pada fasilitas nuklir Natanz milik Iran. Fakta di atas sesuai dengan ketentuan dari Tallinn Manual *Rule 41, Commentary 2*.

Unsur ketiga *MEAN/TOOL* dalam kasus ini, virus stuxnet dalam penggunaannya apabila tidak menggunakan teknologi dan sistem komputer maka virus tersebut bisa dibilang tidak berguna karena stuxnet sendiri terbentuk dari susunan perintah komputer yang dibentuk berupa program komputer yang dapat dijalankan atau diperintah, sehingga ada eksploitasi atau pemanfaatan dari teknologi informasi yang dilakukan oleh negara *uploader* yaitu Amerika Serikat dalam melakukan *cyber operation*-nya. Fakta di atas sesuai dengan ketentuan Tallinn Manual *Rule 41, Commentary 2,* tepat pada pernyataan : "*Cyber means of warfare therefore include any cyber device, materiel, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber attack (Rule 30)."*

Dari analisis di atas dapat disimpulkan bahwa, *malware* jenis worm bernama stuxnet yang dikirim oleh Amerika Serikat untuk menggagalkan pengembangan program nuklir Iran dapat disebut sebagai senjata berdasarkan hukum Humaniter Internasional. Lebih spesifiknya menurut *Tallinn Manual on International Law Applicable To cyberwarfare* virus stuxnet tersebut dapat dikategorikan sebagai *cyber weapon*.

KESIMPULAN

1. *Cyber-attack* yang dilakukan oleh Amerika Serikat terhadap fasilitas nuklir Iran dengan menggunakan virus stuxnet tergolong tindakan Intervensi terhadap Kedaulatan negara Iran. Amerika Serikat melanggar kedaulatan negara Iran di dalam *cyberspace* yang merupakan yurisdiksi negara Iran.

2. Alasan Amerika Serikat melakukan penyerangan dengan alasan mempertahankan diri tidak sesuai dengan prinsip-prinsip umum yang diakui dalam hukum internasional, terutama prinsip *non-use act of force* dan *non-Intervention.* Peraturan berkenaan mengenai prinsip *non-use act of force* dan *non-Intervention* tercantum dalam *United Nation Charter, Chapter I: Purposes And Principles. United Nation Charter Article 2 (4)* dan *Tallinn Manual on International Law applicable to cyber warfare* sendiri mengatur mengenai *Use of Force*, hal tersebut tercantum pada *Chapter II, The Use Of Force, Section I : Prohibition of the use of Force* pada *Rules 10-12.*

3. *Cyber-attack* negara Amerika Serikat sebagai perwujudan dari Doktrin *Pre-emptive military strike* dengan maksud melakukan perlindungan diri dari potensi ancaman Negara Iran mengembangkan teknologi nuklir untuk membuat senjata tidak dapat dibenarkan karena tidak adanya serangan bersenjata dari pihak Iran, sehingga unsur "*if an armed attack occurs"* di dalam ketentuan *United Nations Charter article 51.* tindakan dari Amerika Serikat dan Israel dalam melakukan *Cyber-attack* terhadap Iran memenuhi unsur-unsur dari tindakan Agresi terhadap bangsa lain yang ada pada Resolusi Majelis Umum Perserikatan Bangsa-Bangsa Nomor 3314 (XXIX), artikel 1.

4. Virus stuxnet yang digunakan Amerika Serikat dalam *Cyber-attack* ke Iran dapat disebut sebagai senjata apabila memenuhi ketiga unsur, yaitu :

1) *Context*
2) *Purpose*.
3) *Mean/tool*

Sehingga *Malware* stuxnet dapat dikategorikan sebagai senjata. Lebih spesifiknya menurut *Tallinn Manual on International Law Applicable To cyber warfare, Rule 41, Commentary 2* virus stuxnet tersebut dapat dikategorikan sebagai *Cyber Weapon*.

SARAN

1. Hukum Humaniter Internasional melalui konvensi-konvensinya belum dapat dikatakan sempurna untuk diterapkan dalam kasus *cyber warfare*. Perlu adanya kerjasama dengan para ahli yang memiliki kemampuan dalam bidang teknologi dan informasi serta para ahli dalam bidang hukum humaniter untuk melakukan analisis atau pencarian fakta dalam penyidikan penggunaan *cyber weapon* dalam *cyber warfare* oleh suatu negara, apabila penggunaannya tersebut dikategorikan sebagai tindakan melawan hukum seperti yang dilakukan oleh Amerika terhadap Iran.
2. *Tallinn Manual on international law Applicable To cyber warfare* sebagai petunjuk penerapan hukum internasional dalam cyber warfare agar mendapatkan kekuatan hukum yang sah sebaiknya, perlu segera di tingkatkan statusnya sejajar dengan konvensi melalui kesepakatan dari Negara-negara atau komunitas Internasional.
3. Sulitnya pembentukan definisi dari Agresi di dalam kerangka Statuta Roma 1998, yang disebabkan oleh banyaknya kepentingan politik dari negara-negara anggota PBB, akan membuat kekaburan definisi dari Agresi dan penafsiran yang dilakukan oleh setiap negara yang memiliki kepentingan akan menafsirkannya secara politis, dan akan jarang sekali penafsiran tentang Agresi dilakukan secara Yuridis/ hukum. Padahal apabila dianalisa menurut fungsinya yang menciptakan suatu keadilan dan ketertiban adalah Hukum, sedangkan dari politik belum tentu dapat tercipta keadilan dan ketertiban.

DAFTAR PUSTAKA

SUMBER LITERATUR BUKU :

Arie Siswanto, **Yuridiksi Material Mahkamah Kejahatan Internasiona**l, yudhistira, Bogor, 2005.

Arlina Permanasari dkk, **Pengantar Hukum Humaniter**, ICRC Jakarta, Miamata Print, Jakarta, 1999.

Even, Shmuel, and Siman-Tov, David, ***Cyber warfare: Concepts and Strategic Trends****, Institute For National Security Studies*, 2012.

J.G Starke, **Pengantar Hukum Internasional**, Sinar Grafika, Jakarta, 2000.

Malcolm N. Shaw, **Hukum Internasional**, Nusa media, Bandung, 2013.

Masyhur Effendi, **Hukum Humaniter Internasional Dan Pokok-Pokok Doktrin HANKAMRATA**, Usaha Nasional, Surabaya, 1994.

Peter Mahmud Marzuki, **Penelitian Hukum, Kencana**, Jakarta, 2005.

Solis, Gary D., ***The Law of Armed Conflict****, Cambridge University Press, 2010.*

SUMBER JURNAL :

Kerr, Paul K, *"Iran's Nuclear Program : status", Congressional Research Service Report for Congress*, 2009.

Clark, David, ***Characterizing Cyber space: past, present and future****, MIT CSAIL, 2010.*

Crawford, Emily, ***The Modern Relevance of The Martens Clause****, The University of Sydney, Sydney Law School, 2011.*

Kumar, H.Shravan, **Seminar Report on Study of Viruses and Worms**, KReSIT, I.I.T Bombay

Hayashi, Nobuo, ***Requirement of Military Necessity in International Humanitarian Law and International Criminal Law****, Boston University Internasional Law Journal*, 2010.

Ryant, Rebecca, ***What Kind of Space is Cyber space?****, Minerva-An Internet Journal of Philosophy*, 2001.

Sassoli, Marco, Legitimate Targets of Attack Under International Humanitarian Law, Program on Humanitarian Policy and Conflict Research at Harvard University, 2003.

Schmitt, Michael.N., Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance, Virginia Journal of International Law, 2010.

Shams-us-Zaman, 2011, *Possibility and Implication of Israeli Strike on Iranian Nuclear Installation, National Defense University journal, 2011.*

Stefano Mele, *Legal Considerations of Cyber Weapon, journal of Law and Cyber Weapon* Vol. 3, 2013-2014.

Toukan, Abdullah and Anthony H. Cordesman, *Study on a possible Israeli Strike on Iran's nuclear development Facilities, Centre for Strategic and International Studies*, 2009.

Yaphe, Judith S., and Charles D. Lutes, *Reassesing the Implication of a Nuclear-Armed Iran, Institute for National Strategic Studies, National Defense University* : Washington D.C, 2005.

SUMBER PERATURAN PERUNDANG-UNDANG :

Additional Protocol To The Geneva Conventions Of 12 August 1949, And Relating To The Protection Of Victims Of International Armed Conflicts (Protocol I), 8 June 1977.

Budapest Convention on Cybercrime 2001.

Convention III Relative To The Treatment Of Prisoners Of War. Geneva, 12 August 1949.

Convention (V) Respecting The Rights And Duties Of Neutral Powers And Persons In Case Of War On Land. The Hague, 18 October 1907.

Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX).

Rome Statute on Human Rights 1998.

Tallinn Manual On The International Law Applicable To Cyber warfare.

The Geneva Convention And Relating To The Protection Of Victims Of International Armed Conflicts 12 August 1949.

*Treaty For The Prohibition Of Nuclear Weapons In Latin America And The Caribbean/*Treaty Of Tlatelolco.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

United Nations Charter.

SUMBER INTERNET :

*Chad Nelson, **Cyber warfare: The Newest Battlefield**, Washington University in St. Louis, http://www.cse.wustl.edu/~jain/cse571-11/ftp /cyberwar.pdf* (12 Oktober 2013)

Darrel Menthe, *Jurisdiction In Cyberspace : A Theory of International Spaces, MICH.TELECOMM.TECH.L.REV* 69, 1998, *http://www.mtlr.org/volfour/menthe.html*. (30 Oktober 2014)

Grimmett F. Richard , 2003, U.S. Use of preemptive Military Force, CRS Report for congress, www.fas.org/man/crs/RS21311.pdf (12 Maret 2014)

Juliet M. Oberding, ***A Separate Jurisdiction For Cyberspace?,*** *http://www.oberding.com/-juliet/resources.html* (28 oktober 2014)

Kuehl, Dan, From Cyber space to Cyberpower: Defining the Problem, Information Operations at the National Defense University, USA, www.carlisle.army.mil/DIME/documents/ (20 Februari 2013)

Sanger, David. E., 2012, Obama Order Sped Up Wave of Cyber attacks Against Iran, The New York Times: Middle East, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave- of-Cyber attacks-against iran.html?_r=2& (25 maret 2013)

Nils Melzer, 2011, ***Cyber warfare and International Law****, UNIDIR. RESOURCES. IDEAS FOR PEACE AND SECURITY, unidir.org/pdf/activites/pdf2-act649.pdf* (15 maret 2014)

See speeches of President George W. Bush at West Point on June 1, 2002 at [http://www.whitehouse.gov/news/releases/2002/06/20020601-3.html]; (25 Maret 2013)

Washington Post, June 2, 2002, p. A1; Washington Post, September 13, 2002, p.A1. The National Security Strategy of the United States of America is found at [http://www.whitehouse.gov/nsc/nss.html]. (25 Maret 2013)