MAJALAH ILMU HUKUM
KERTHA WICAKSANA

IAWAN SOERODJO
Hak Pengelolaan Atas Tanah Sebagai Jaminan

JANI HARTANTO
Aspek Hukum Waralaba Restoran

OKY DEVIANY BURHAMZAH
Campur Tangan Pemerintah Dan Pengaturan Hukum
Persaingan Usaha Dalam Pembangunan Perkonomian Nasional

NLM MAHENDRAWATI DAN IB GEDE AGUSTYA MAHAPUTRA
Eksekusi Hak Tanggungan Oleh Bank Terhadap Jaminan
Kredit Nasabah Yang Cedera Janji

URIP SANTOSO
Sewa Menyewa dan Jual Beli Tanah Pemerintah
Kabupaten/Kota Dalam Peraturan Pemerintah Nomor 6 Tahun 2006

AGUS MULYAWAN
Pembentukan Peraturan Daerah Provinsi Yang Aspiratif
Dalam Konteks Penyelenggaraan Otonomi Daerah

HIMAWAN ESTU BAGIJO
Perumusan Norma dan Sanksi Administrasi Dalam
Pembentukan Peraturan Perundang-undangan

NYOMAN SUTAMA dan NYOMAN SUMARDIKA
Izin Lingkungan Sebagai Instrumen Perlindungan dan
Pengelolaan Lingkungan Hidup

CAYOTREM
Peran Hak Asasi dan Aliran-Aliran Dalam Paradigma Ilmiah
Bagi Metodologi Riset
Dalam Kerangka Pengembangan Kemajuan Tekno-science

LILIK MULYADI
Implementasi Atas pembalikan Beban Pembuktian Pada
Praktik Perkara Tindak Pidana Kerupsi di Negara Hongkong
dan India

MASKUN, ALMA MANUPUTTY, S.M. NOOR, dan
JUahir SUMARDI
Siber Teroris : Genus Baru Dalam Hukum Kejahatan
Internasional

SIMON NAHAk
Kebijakan Mediasi Penal Terhadap Penyelesaian Pelaku
Tindak pidana Bidang Perpajakan Oleh Wajib Pajak dan
Pihak Ketiga di Indonesia

A.A.SAGUNCULAKSMIDewi
Upaya Hakim Terhadap Putusan Prosedur Dismissal Dalam
Sengketa di Peradilan Tata Usaha Negara

DAI AYUTRY PUSPA
Hukum Hindu Dalam Waris Perempuan di Bali

IKetut SUKADANA
Pemutusan Kedewasana Dalam Perkawinan Menurut
Hukum Adat Bali

Volume 19 Nomor 3 September 2013
Halaman 248 - 368
MAJALAH ILMU HUKUM
KERTHA WICAKSANA

ISSN 0853-6422

PENANGGUNGJAWAB:
Ni Luh Made Mahendrawati

DEWAN EDITOR:
I Gusti Bagus Suryawan (Ketua)
Ni Made Puspasutari Ujiyanti (Sekretaris).
Luh Putu Suryani (Bendahara)
Ni Komang Arini Styawati (Anggota)
AA Sagung Laksmi Dewi (Anggota)
Diah Gayatri Sudibya (Anggota)
I Wayan Arthanaya (Anggota)
Isnri Rubiantini (Anggota)

TATA USAHA:
Ni Made Surya
I Wayan Suja
I Nyoman Eka
Ni Nyoman Yuli
I Nyoman Sidarta
I Gusti Ayu Kwi.

SEKRETARIAT:
Fakultas Hukum Universitas Warmadewa Denpasar
Jl. Terompong No. 24 Tanjung Bungkah Denpasar (60235)
Telp (0361) 223858 (hunting), 7449633, Fax (0361) 263902
E-mail: kerthawicaksana@yahoo.co.id

MAJALAH ILMU HUKUM KERTHA WICAKSANA
diterbitkan oleh Fakultas Hukum Universitas Warmadewa Denpasar
bekerjasama dengan Ikatan Notaris Indonesia (INI) Bali
dan Perhimpunan Advokat Indonesia (PERADI) Denpasar sebagai Media Informasi
dan Pengembangan Ilmu Hukum, yang diterbitkan dua kali setahun
yaitu setiap bulan Januari dan Juli.

Berdasarkan Keputusan Direktur Jenderal Pendidikan Tinggi Kementerian Pendidikan
Nasional Nomor : 64a/DIKTI/Kep./2010, Majalah Ilmu Hukum Kertha Wicaksana
dinyatakan terakreditasi sebagai Jurnal Ilmiah Nasional
EDITORIAL


Dengan beragamnya artikel pada edisi ini, diharapkan dapat bermanfaat dan semakin menambah wawasan bagi pembaca yang budiman.

Selamat membaca

Dewan Redaksi
DAFTAR ISI

EDITORIAL ................................................................. i
DAFTAR ISI ................................................................... ii

HUKUM BISNIS DAN KENOTARIATAN
IRAWAN SOERODJO
Hak Pengelolaan Atas Tanah Sebagai Jaminan ............................ 248
J ANDI HARTANTO
Aspek Hukum Waralaba Restoran ............................................. 254
OKY DEVIANY BURHAMZAH
Campur Tangan Pemerintah Dan Pengaturan Hukum Persaingan Usaha Dalam Pembangunan Perekonomian Nasional ......................... 262
NLM MAHENDRAWATI DAN IB GEDE AGUSTYA MAHAPUTRA
Eksekusi Hak Tanggungan Oleh Bank Terhadap Jaminan Kredit Nasabah Yang Cederai Janji .............................................. 273

HUKUM PEMERINTAHAN
URIP SANTOSO
Sewa Menyewa dan Jual Beli Tanah Pemerintah Kabupaten/Kota Dalam Peraturan Pemerintah Nomor 6 Tahun 2006 .......................... 279
AGUS MULYAWAN
Pembentukan Peraturan Daerah Provinsi dan Daerah Perbatasan Dalam Konteks Penyelenggaraan Otonomi Daerah ................................................. 290
HIMAwan ESTU BAGIJO
Perumusan Norma dan Sanksi Mundur dan Dalam Penentuan Peraturan Perundang-undangan .................................................. 301
NYOMAN SUTAMA dan NYOMAN DEWANTA
Izin Lingkungan Sebagai Instrument Penentuan dan Pengelolaan Lingkungan Hidup ......................................................... 314
I MADE GOTREM
Peranan Filsafat dan Aliran-Aliran Dalam Paradigma Ilmu Bagi Metodologi Riset Dalam Kerangka Pengembangan Kemajuan Technoscience ................................................................. 319

KEPENGACARAAN
LILIK MULYADI
Implementasi Atas pembalikan Beban Pembuktian Pada Praktik Perkara Tindak Pidana Korupsi di Negara Hongkong dan India ...................................................... 326
MASKUN, ALMA MANUPUTTY, S.M. NOOR, dan JUAJIR SUMARDI
Siber Teroris : Genus Baru Dalam Hukum Kejahatan Internasional ................................................................. 334
SIMON NAHAk
Kebijakan Mediasi Penal Terhadap Penyelesaian Pelaku Tindak pidana Bidang Perpajakan Oleh Wajib Pajak dan Pihak Ketiga di Indonesia ............................................. 341
A.A SAGUNG LAkSMI DEWI
Upaya Hukum Terhadap Putusan Prosedur Dismissal Dalam Sengketa di Peradilan Tata Usaha Negara ................................................................. 1351

PENGENEBANGAN HUKUM LOKAL
IDA AYU TARY PUSPA
Hukum Hindu Dalam Waris Perempuan di Bali ........................................ 356
I KETUT SUKADANA
Penentuan Kedewasaran Dalam Perkawinan Menurut Hukum Adat Bali ................................................................. 363

INDEKS PENULIS .................................................................. 389
INDEKS SUBYEK .................................................................. 370
UCAPAN TERIMAkasIH .......................................................... 371
DAFTAR KEGIATAN ILMIAH ..................................................... 372
PETUNJK PENULISAN ........................................................... 373
SIBER TERORIS: GENUS BARU HUKUM KEJAHATAN INTERNASIONAL

(CYBER TERRORISM: A NEW GENUS OF INTERNATIONAL CRIMINAL LAW)

Maskun, Alma Manuputty, S.M. Noor, Juajir Sumardi

International Law Department, Hasanuddin University, Makassar
Jl. Perintis Kemerdekaan Km. 10, Tamalanrea, 90245
maskunlawschool@yahoo.co.id

ABSTRAK


Kata Kunci: Siber Terrorism, Siber Aggressor, dan Ancaman Terrorism

ABSTRACT

Cyber terrorism is a fact. It is real and immediate. The traditional modus of the terrorism has been developed by terrorists to apply computer and internet (cyber) as the tool to do "terror". The terrorist websites can serve as virtual training grounds, offering tutorials on building bombs, surface-to-air missile operation, surveillance, intelligence gathering and operational security. Terrorists have also developed sophisticated encryption tools and creative techniques that render the Internet an efficient and relatively secure means of correspondence. Computers and servers are the most aggressively targeted information systems in the world, with attacks increasing in severity, frequency, and sophistication each year. The fact shows us that the use of information, communication, and technology (ICT) is becoming something very important for countries all over the world to do their activities. These cyber-aggressors can threaten not only nation's economy and public works but also communication systems and computer networks. In terms of prosecution of the perpetrator, it refers to S.C. Res. 1371 (2001) and S.C. Res. 1566 (2004), as well as national law of state. Indeed, it has to consider to the "mens rea" and "the actus rea" of the crime have been developed to reach out of the law.

Keywords: Cyber Terrorism, Cyber Aggressor, Threat of Terrorism

INTRODUCTION

Terrorism has become "a hot issue" since the September 11 attack (Walter Lanquer, 2001: 71). It is becoming a global phenomenon which threatens all countries but it is not a new phenomenon (Sapto Waluyo, 2007:112). Not a new phenomenon means that the 11 September accumulated all motives around the world such as the global economy, ideological and religious motives (Walter Lanquer, 2001:10-13).

The problem of terrorism basically is long-rooted in human history and has been changed nowadays in terms of modus, tactic, strategy and use of technology as its tools to commit terror. Related to the use of technology, the traditional modus of the terrorism has been developed by terrorist (attackers) to apply computer and internet (cyber) as the tool to commit their "terror". The terrorist use it to recruit its members, to get financial supporting (fundraising), to promulgate its ideologies and
ideas, and to plan, coordinate and publicize its organization or a workplace as for a group engaged in criminal activities (Clare Crildland, 2008: 5). The website can serve as virtual training grounds, offering tutorials on building bombs, surface-to-air missile operation, surveillance, intelligence gathering and operational security. The terrorists (attackers) have also developed sophisticated encryption tools and creative techniques that render the internet an efficient and relatively secure means of correspondence.

The use of technology as a new basis of the terrorist to commit the terror as mentioned above actually bear “cyber terrorism” as development of terrorism and part of cyber crime in literature of international criminal law. Indeed, the development of concept and modes of terrorism and part of cyber crime bring a lot of problem particular in terms of law enforcement. This is taking place because the law concerning terrorism either international, regional, or national does not regulate clearly if the terror is applying technology although element of crime of terrorism is fitted.

The threat of cyber-terrorism is real and immediate. Computers and servers are the most aggressively targeted information systems in the world, with attacks increasing in severity, frequency and sophistication each year. The fact shows that the use of information, communication, and technology (ICT) is being something very important for countries all over the world to do their activities. These cyber-aggressors can threaten not only nation’s economy and public works but also communication systems and computer networks.

Therefore, discussion of this paper will focus on cyber terrorism as a new genus of international criminal law specifically how to prosecute the perpetrator (the aggressor/terrorist) specifically the “mens rea” and “the actus rea” of the crime when there is no the laws against of terrorism based on using technology as a tools? However, before discussing deeply, I would like to define the meaning of terrorism in order to connect to the meaning of cyber terrorism.

**ANALYSIS**

**The Meaning of Terrorism and Cyber Terrorism**

To define terrorism is not an easy task. Some scholars are facing some difficulties to define it because of considerable disagreement of definition of terrorism. According to Craig Stapley (2009:15), “a quick review of the literature shows that there is no accepted definition in government or in academia”. Kushner (2003: xxiii) furthermore notes that “there are as many definitions for the word terrorism as there are methods of executing it; the term means different things to different people, and trying to define or classify terrorism to everyone’s satisfaction proves impossible.” Louise Richardson (2003) also stipulates that “the widespread usage of the term terrorism, in many contexts, has rendered the word almost meaningless. Today, it’s only universally understood connotation is so pejorative that even terrorists don’t admit to being terrorists any more. A glance at the current usage reveals child abuse, racism, and gang warfare all incorrectly described as terrorism”.

The difficulties of definition term of terrorism as stated above can be understood both theoretically and practically. Even, in the United Nations Security Council Resolution 1373 (2001) does not mention definition of it. As we know, the SC Resolution 1373 (2001) is one of the pillars of the global legal framework for the prevention and suppression of terrorism (Walter Gehr, 2004: 101-101). It refers to the binding upon member states of the General Assembly. Its position then plays an important role to fight against the terrorism.

However, difficulties to define it, it does not mean that we can merely to define it based on what they want to define as terrorism. A clear definition of terrorism has to be tried to be defined because of some essential reasons such as “in any systematic study of a phenomenon, it is necessary to have discrete definitions of the items being studied in order to ensure consistent and valid conclusions. It is especially important to have a concrete definition when there is no clear consensus as to what is or is not terrorism” (Craig Stapley, 2009: 15).

Some definition can be traced in some literature to see various meaning of terrorism. Terrorism can be defined as “the threat or the act of politically violence directed primarily against civilian” Graeme C.S. Steven and Rohan Gunaratna, (2004:7). CIA also has its own definition concerning terrorism, it defines terrorism as “the threat or use of violence for political purposes by individuals or groups, whether action for, or in opinion to established governmental authority, when such actions are intended to shock or intimidate at target group
wider than the immediate victims” (Bambang Abimanyu, 2005:130).

FBI itself states terrorism as “the unlawful use of force or violence against persons or property to intimidate or coerce government, civilization populations, or any segment threat, in furtherance of political or social objective (Bambang Abimanyu, 2005:130). US Army Operational Concept for Terrorism Counteraction notes that terrorism constitutes “the calculated use of violence or threat of violence to attain goals that are political, religious, or ideological in nature... through intimidate, coercion, or instilling fear” (Bambang Abimanyu, 2005:131).


Those terrorism definition as defined previously has connection to meaning of cyber terrorism. The basic concept of terrorism basically does not change but it has added some elements of crime, as result of using of technologies as the terrorist tool. According to Jason Andress, et.al (2011: 198-199), cyber terrorism is “a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda”.

Similarly to Andress, R. Ahmad and Z. Yunus (2012:149), indicates that cyber terrorism has several attributes such as motivation, impact, and target. R. Ahmad, et.al (2012:232) furthermore explains that term motivation means political, ideological and social; Impact itself refers to mass destruction or seriously interfere critical services operation, cause fear, death or bodily injury, and severe economic loss; and, target is driven to critical national infrastructure computer system and civilian population.

In terms of definition or meaning of terrorism and cyber terrorism as explained above, it can be concluded that there is similarity both meaning of them in some crucial elements such as violence, creating fear, and its target civilian. If in the past, cyber terrorism had been thought as threat in future as mentioned by Andrew Rathmell (1997 : 140), so less than 10 year after his question, cyber terrorism is being a fact and it cannot be wished away. Corporations, government, and private citizen are all at risk and equally all are responsible for preventing and fighting such attacks (Albert J. Marcella, 2000:: 10). All possibilities risks is producing fear in people daily life. It is because people tend to be afraid to something they do not see (invisible) and they do not understand (Ananda Mitra, 2010:55), (Michael Stohl, 2006:225).
Actus Reus and Mens Rea of Cyber Terrorism

To decide elements of crime of cyber terrorism basically refers to definition of cyber terrorism. Even though, there is no clear definition of it that has been agreed, it is very important to see element of terrorism as noted in to Security Council Resolution 1371 (2001) concerning Antiterrorism Resolution and Security Council Resolution 1566 (2004) concerning threats to international peace and security caused by terrorism. The explaining elements of crime of terrorism can be used because of function of the Security Council Resolution is legally binding for UN members. For the purposes of this analysis therefore, I quote those elements as elements crime of cyber terrorism because in "reaffirming of that Resolution stated that "terrorism in all its forms and manifestations constitutes one of the most serious threat to peace and security". It is also because in Paragraph 3 point (a) S. C. Res. 1371 (2001) stated "...intensifying and accelerating the exchange of operational information, especially regarding actions or movements of terrorist persons or networks, and the use of communication technologies by terrorist groups...".

Actus reus theoretically consists of two elements. Actus reus refers to whether he/she conduct a crime. Mens rea is commonly referred as a mental element of crime. Mens rea is the objective intent of perpetrator to commit a crime that may be formed in terms of intention or neglect. Mens rea is called as a subjective element of crime.

Actus reus of cyber terrorism refers to the Security Council Resolution 1373 (2001) in Paragraph 3, as followings: 1. To exchange operational information especially regarding actions or movements of terrorist persons or networks; 2. To forge or falsify travel documents; 3. To traffic in arms; 4. To use explosives or sensitive materials; and 5. To use communication technologies.

Paragraph 3 to the Security Council Resolution 1566 (2004) stated furthermore actus reus of it, as followings (Walter Gehr, 2004: 104): 1. To cause death or serious bodily injury or taking hostages; 2. To provoke a state off terror in the general public or in group persons or particular person; 3. To intimidate a population; 4. To compel a government or an international organization to do or to abstain... which constitutes offence within the scope of and as defined... relating to terrorism...."

Both S.C. Res actually had covered element of crime of cyber terrorism (actus reus) indirectly. However, to complete actus reus of cyber terrorism is necessary to put "the use of computers and telecommunications capabilities as an important element to convergence between cyberspace and terrorism.

The crime also requires criminal intent to be classified as crime. Related to it, mens rea of cyber terrorism is put into intention and knowledge of the perpetrator (terrorist). Intent of the perpetrator (terrorist) means that they have motive in political, social or religious in nature. (Dean Alexander, 2012:79) Whereas knowledge means that they know fluently how to do terror and the effect is coming from the terror in which they generally do not care about their victims.

One of the forms of knowledge of the perpetrators can be found in purpose of the terror. The perpetrators generally realize that what they do (terror) will create fear as noted also in traditional modus of terrorism (P. Flemming and Michael Stohl, 2001:70). In terms of fear, cyber terrorism conveys two significant modern fears: the fear of technology and the fear of terrorism. Both the fear of technology and the fear of terrorism are visible and difficult to be understood. This can create cyberfear that is generated by cyberterrorists that what a computer/internet attack will bring down airliners, ruin critical infrastructure, destroy the stock market, reveal an arms planning secret, etc.

T.L. Thomas, 2001

Prosecution of Cyber Aggressors (the Perpetrators/Terrorists)

Prosecution of cyber terrorism will be governed under the same regulation to prosecution of terrorism. Even though there is no exactly definition that is agreed by all states worldwide and scholars/experts, it can be used interpretation to cover cyber terrorism. Pursuant to Article 31 of Vienna Convention 1969, "a treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to terms of the treaty in their context and in the light of its object and purpose".

According to Rebecca M.M. Wallace (1992:228-229), there are 3 (three) main approaches in international law to treaty interpretation. First, the objective approach — interpretation in accordance with the ordinary use of the words of the treaty; Second,
subjective approach - interpretation in accordance with the intention of the parties to the treaty; and third, the teleological approach - interpretation in accordance with treaty’s aims and objectives.

Those approaches as noted by Wallace can be applied to interpret actus reus and mens rea terrorism to cyber-terrorism as mentioned above. Article 31 of Vienna Convention 1969 furthermore is deemed as “an umbrella law” for covering cyber terrorism, particular in some resolution as indicated in S.C.Res. 1373 (2001), S.C.Res. 1534 (2004), S.C.Res. 1566 (2004) and other S.C.Res. governing terrorism or related to terrorism. They generally oblige to “a state” to counter terrorism in all aspects and issues. The meaning obligation of counter terrorism to “state” is all state shall take control for all terrorism activities in its territory either conducted by a person, a group, or a state. It is therefore that it is pivotal for all countries to have their own laws to deal with terrorism issues, including dealing with law enforcement to the perpetrators (the terrorists).

The terrorism’s perpetrator can be prosecuted not only based on national law but also based on national law of the state. For example, Indonesia, its regulation of counter terrorism is regulated in Anti-Terrorism Law of Republic No. 15 year 2003 concerning an Act of a Government Regulation in the Field of on Terrorism (Number 1/2002). The Law Anti Terrorism Law authorized security officers to arrest and question terrorist suspects based on intelligence information, detain suspects based on sufficient evidence, close the bank account held by the suspects, open personal mail/documents and tap telephone/communication lines.

In terms of prosecution of the perpetrator, it is governed under article 25 of the Law No. 15 year 2003. The article of the Law No. 15 year 2003 basically governs all perpetrators’ (terrorists) conduct as if mentioned in actus reus and mens rea above, including cyber-terrorism. This regulation was applied for the first time to track down the perpetrators (terrorists) of Bali bombing and then it was adopted as a law for all terrorism cases.

In Unites States itself, regulation of use internet can be seen in the first federal computer crime statute was the Computer Fraud and Abuse Act of 1984 (CFAA). The CFAA is the most important computer crime statute in the US because almost every other statute that deals with computer crime modifies the CFAA. The CFAA makes many acts that are associated with cyber-terrorism punishable under US Law. While it does not address the more technical side of cyber-terrorism such as DDoS Attacks, it does address data theft, which, if carried out under the right motives can be associated with cyber terrorism. Also, under Section 1030(a)(2) and (7), the financing of terrorism could possibly be prosecuted under this act (Maxim May, 2004:2).

There is also Federalist No. 10 that agrees not only to the internet’s use but also can be significant assistance to the US campaign against transnational terrorism (Dawinder S. Sidhu, 2010: 3-5). The Federalist mentions that online and mobile media are becoming an integral and part of everyday lives in which computer plays a significant role in data storage and plenty of sensitive personal and institutional information are stored as digital data, particular for national security data. One of cyber terror was at first suspected in the 2003 Northeast blackout, even though it did not attack US military capabilities and US economy. Other examples of imminent terrorist attacks via the Internet can be found in “Electronic Pearl Harbor” or “Digital Waterloo.”

In India, there is India’s Information Technology Act (I.T.A.) of 2000 that addresses the illegal use of the Internet and enables the government of India to prosecute against offences that are associated with cyber terrorism including DDoS attacks. The I.T.A. of 2000 takes into account the understanding that the right to privacy is part of the right to life and personal liberty enshrined under Article 21 of the Constitution of India. The Indian Cyber Crimes Legislation also deals specifically with cyber attacks or recent legislation from the U.S. House of Representatives dealing specifically with cyber terrorism (Praveen Dalal, 2006).

Those national regulations of counter terrorism as mentioned above are purpose to prosecute the perpetrators. This is because without punishment, it is difficult to diminish terror including cyber terror or to fight against cyber terrorism.

**CONCLUSION**

It can be concluded that cyber terrorism is present threat. It has some elements to be fulfilled in order to be categorized as a crime of cyber terrorism. Those elements are qualified as actus reus and mens rea of cyber terrorism.
Both actus reus and mens rea require unlawful means as method of action; network warfare and psychological operation as tools of attack; political, ideological, social and cultural as motivation; critical national infrastructure computer system and civilian population as targets; mass disruption or seriously interfere critical services operation, cause fear, death or bodily injury, and severe economic loss as impact negatively, and cyberspace as domain.

When both actus reus and mens rea are fulfilled, the perpetrators (terrorists) can be prosecuted either applying international law instrument as if Security Council Resolution or national law of states like the Law No. 15 year 2003 concerning Enacting of a Government Regulation in lieu of Law on Terrorism Number 1/2002, some laws in US and India.

REFERENCES


Lowther and Beverly Lindsay, *Terrorism’s Unanswer Questions*, London: Greenwood Publishing Group.


MAJALAH ILMU HUKUM
KERTHA WICAKSANA

Volume 19 Nomor 3 September 2013
Halaman 248 - 368

IRAWAN SOERODJO
Hak Pengelolaan Atas Tanah Sebagai Jaminan

JANDI HARTANTO
Aspek Hukum Waralaba Restoran

OKY DEVIANY BURHAMZAH
Campur Tangan Pemerintah Dan Pengaturan Hukum Persaingan Usaha Dalam Pembangunan Perekonomian Nasional

NLM MAHENDRAWATI DAN IB GEDE AGUSTYA MAHAPUTRA
Eksekusi Hak Tanggungan Oleh Bank Terhadap Jaminan Kredit Nasabah Yang Cederai Janji

URIP SANTOSO
Sewa Menyewa dan Jual Beli Tanah Pemerintah Kabupaten/Kota Dalam Peraturan Pemerintah Nomor 6 Tahun 2006

AGUS MULYAWAN
Pembentukan Peraturan Daerah Provinsi Yang Aspiratif Dalam Konteks Peningkatan Otonomi Daerah

HIMAWAN ESTU BAGIJO
Perumusan Norma dan Sanksi Administrasi Dalam Pembentukan Peraturan Perundang-undangan

NYOMAN SUTAMA dan NYOMAN SUMARDIKA
Izin Lingkungan Sebagai Instrumen Perlindungan dan Pengelolaan Lingkungan Hidup

JAPRI GOREM
Pemetaan Perubahan dan Aliran-Aliran Dalam Paradigma Ilmiah Bagi Metodologi Riset Dalam Kerangka Pengembangan Kemanajemen Teknokratia

LILIK MULYADI
Implementasi Atas pembalikan Beban Pembuktian Pada Praktik Perkara Tindak Pidana Kerupsi di Negara Hongkong dan India

MASKUN, ALMA MANUPUTTY, S.M. NOOR, dan JUJURISUMADI
Siber Teroris : Genus Baru Dalam Hukum Kejahatan Internasional

SIMO NAHAK
Kebijakan Mediasi Penal Terhadap Penyelesaian Pelaku Tindak pidana Bidang Perpajakan Oleh Wajib Pajak dan Pihak Ketiga di Indonesia

AASAGUNG LAKSMI DEWI
Upaya Hakim Terhadap Putusan Prosedur Dismissal Dalam Sengketa di Peradilan Tata Usaha Negara

IDA AYUTARIY PUSPA
Hukum Hindu Dalam Waris Perempuan di Bali

IKETUT SUKADANA
Pemenuhan Kedewasaan Dalam Perkawinan Menurut Hukum Adat Bali
MAJALAH ILMU HUKUM KERTHA WICAKSANA
ISSN 0853-6422

PENANGGUNGJAWAB:
Ni Luh Made Mahendrawati

DEWAN EDITOR:
I Gusti Bagus Suryawan (Ketua)
Ni Made Puspasutari Ujiyanti (Sekretaris).
Luh Putu Suryani (Bendahara)
Ni Komang Arini Styawati (Anggota)
AA Sagung Laksmi Dewi (Anggota)
Diah Gayatri Sudibya (Anggota)
I Wayan Arthanaya (Anggota)
Isnri Rubiantini (Anggota)

TATA USABA:
Ni Made Surya
I Wayan Surya
I Nyoman Ketut
Ni Nyoman Ketut
I Nyoman Sudibya
I Gusti Ayu Keli

SEKRETARIAT:
Fakultas Hukum Universitas Warmadewa Denpasar
Jl. Terompong No. 24 Tanjung Bungkah Denpasar (60235)
Telp (0361) 223858 (hunting), 7449633, Fax (0361) 263902
E-mail: kerthawicaksana@yahoo.co.id

MAJALAH ILMU HUKUM KERTHA WICAKSANA
diterbitkan oleh Fakultas Hukum Universitas Warmadewa Denpasar
bekerjasama dengan Ikatan Notaris Indonesia (INI) Bali
dan Perhimpunan Advokat Indonesia (PERADI) Denpasar sebagai Media Informasi
dan Pengembangan Ilmu Hukum, yang diterbitkan dua kali setahun
yaitu setiap bulan Januari dan Juli.

Berdasarkan Keputusan Direktur Jenderal Pendidikan Tinggi Kementerian Pendidikan
Nasional Nomor: 64a/DIKTI/Kep./2010, Majalah Ilmu Hukum Kertha Wicaksana
dinyatakan terakreditasi sebagai Jurnal Ilmiah Nasional
EDITORIAL


Dengan beragamnya artikel pada edisi ini, diharapkan dapat bermanfaat dan semakin menambah wawasan bagi pembaca yang budiman.

Selamat membaca

Dewan Redaksi
DAFTAR ISI

EDITORIAL ........................................................................................................................................ i
DAFTAR ISI ....................................................................................................................................... ii

HUKUM BISNIS DAN KENOTARIATAN
IRAWAN SOERODJO
Hak Pengelolaan Atas Tanah Sebagai Jaminan ................................................................................. 248
J ANDI HARTANTO
Aspek Hukum Waralaba Restoran .................................................................................................... 254
OKY DEVIANY BURHAMZAH
Campur Tangan Pemerintah Dan Pengaturan Hukum Persaingan Usaha
Dalam Pembangunan Perekonomian Nasional .................................................................................. 262
NLM MAHENDRAWATI DAN IB GEDE AGUSTYA MAHAPUTRA
Eksekusi Hak Tanggungan Oleh Bank Terhadap Jaminan Kredit Nasabah
Yang Cederan Janji .......................................................................................................................... 273

HUKUM PEMERINTAHAN
URIP SANTOSO
Sewa Menyewa dan Jual Beli Tanah Pemerintah Kabupaten/Kota
Dalam Peraturan Pemerintah Nomor 6 Tahun 2006 ........................................................................... 279
AGUS MULAYAWAN
Pembentukan Peraturan Daerah Pemecahan Perguruan Tinggi dalam Konteks Penyelenggaraan
Otonomi Daerah ..................................................................................................................................... 290
HIMADEVAN ESTU BAGIJO
Perumusan Norma dan Sanksi dalam Undang-undang Peraturan
Peraturan Perundang-undangan ........................................................................................................ 301
NYOMAN SUTAMA dan NYOMAN MAHENDRAWATI
Izin Lingkungan Sebagai Instrument Kehidupan dan Pengelolaan Lingkungan Hidup .......... 314
I MADE GOTREM
Peranan Filsafat dalam Aliran-ALiran Dalam Paradigma Ilmah Bagi Metodologi Riset
Dalam Kerangka Pengembangan Kemajuan Technoscience ............................................................ 319

KEPENGACARAAN
LILIK MULYADI
Implementasi Atas pembalikan Beban Pembuktian Pada Praktik Perkara
Tindak Pidana Korupsi di Negara Hongkong dan India ................................................................ 326
MASKUN, ALMA MANUPUTTY, S.M. NOOR, dan JUAINIR SUMARDI
Siber Teroris : Genus Baru Dalam Hukum Kejahatan Internasional ..................................................... 334
SIMON NAHAK
Kebijakan Mediasi Penal Terhadap Penyelesaian Pelaku Tindak pidana Bidang Perpajakan
Oleh Wajib Pajak dan Pihak Ketiga di Indonesia .............................................................................. 341
AA SAGUNG LAKSMI DEWI
Upaya Hukum Terhadap Putusan Prosedur Dismissal Dalam Sengketa
di Peradilan Tata Usaha Negara ........................................................................................................ 1351

PENGEMBANGAN HUKUM LOKAL
IDA AYU TARY PUSPA
Hukum Hindu Dalam Waris Perempuan di Bali .............................................................................. 356
I KETUT SUKADANA
Penentuan Kedewasaan Dalam Perkawinan Menurut Hukum Adat Bali ........................................... 363

INDEKS PENULIS ................................................................................................................................... 369
INDEKS SUBYEK .................................................................................................................................... 370
UCAPAN TERIMA KASIH ....................................................................................................................... 371
DAFTAR KEGIATAN ILMIAH .................................................................................................................... 372
PETUNJUK PENULISAN .......................................................................................................................... 373
SIBER TERORIS: GENUS BARU HUKUM KEJAHATAN INTERNASионаL

(CYBER TERRORISM: A NEW GENUS OF INTERNATIONAL CRIMINAL LAW)

Maskun, Alma Manuputy, S.M. Noor, Juahir Sumardi

International Law Department, Hasanuddin University, Makassar
Jl. Perintis Kemerdekaan Km. 10, Tamalanrea, 90245
maskunlaw@school@yahoo.co.id

ABSTRAK


Kata Kunci: Siber Terrorism, Siber Aggressor, dan Ancaman Terrorism

ABSTRACT

Cyber terrorism is a fact. It is real and immediate. The traditional modus of the terrorism has been developed by terrorists to apply computer and internet (cyber) as the tool to do "terror". The terrorist websites can serve as virtual training grounds, offering tutorials on building bombs, surface-to-air missile operation, surveillance, intelligence gathering and operational security. Terrorists have also developed sophisticated encryption tools and creative techniques that render the Internet an efficient and relatively secure means of correspondence. Computers and servers are the most aggressively targeted information systems in the world, with attacks increasing in severity, frequency and sophistication each year. The fact shows us that the use of information, communication, and technology (ICT) is being something very important for countries all over the world to do their activities. These cyber-aggressors can threaten not only nation's economy and public works but also communication systems and computer networks. In terms of prosecution of the perpetrator, it refers to SC Res 1371 (2001) and SC Res 1566 (2004), as well as national law of state. Indeed, it has to consider to the "mens rea" and "the actus rea" of the crime have been developed to reach out of the laws.

Keywords: Cyber Terrorism, Cyber Aggressor, Threat of Terrorism

INTRODUCTION

Terrorism has become "a hot issue" since the September 11 attack (Walte Lanquer, 2001: 71). It is becoming a global phenomenon which threatens all countries but it is not a new phenomenon (Sapto Waluyo, 2007:112). Not a new phenomenon means that the 11 September accumulated all motives around the world such as the global economy, ideological and religious motives (Walter Lanquer, 2001:10-13).

The problem of terrorism basically is long-rooted in human history and has been changed nowadays in terms of modus, tactic, strategies and use of technology as its tools to commit terror. Related to the use of technology, the traditional modus of the terrorism has been developed by terrorist (attackers) to apply computer and internet (cyber) as the tool to commit their "terror". The terrorist use it to recruit its members, to get financial supporting (fundraising), to promulgate its ideologies and
ideas, and to plan, coordinate and publicize its organization or a workplace as for a group engaged in criminal activities (Clare Cridland, 2008: 5). The website can serve as virtual training grounds, offering tutorials on building bombs, surface-to-air missile operation, surveillance, intelligence gathering and operational security. The terrorists (attackers) have also developed sophisticated encryption tools and creative techniques that render the internet an efficient and relatively secure means of correspondence.

The use of technology as a new basis of the terrorist to commit the terror as mentioned above actually bear “cyber terrorism” as development of terrorism and part of cyber crime in literature of international criminal law. Indeed, the development of concept and modes of terrorism and part of cyber crime bring a lot of problem particular in terms of law enforcement. This is taking place because the law concerning terrorism either international, regional, or national does not regulate clearly if the terror is applying technology although element of crime of terrorism is fitted.

The threat of cyber-terrorism is real and immediate. Computers and servers are the most aggressively targeted information systems in the world, with attacks increasing in severity, frequency and sophistication each year. The fact shows that the use of information, communication, and technology (ICT) is being something very important for countries all over the world to do their activities. These cyber-aggressors can threaten not only nation’s economy and public works but also communication systems and computer networks.

Therefore, discussion of this paper will focus on cyber terrorism as a new genus of international criminal law specifically how to prosecute the perpetrator (the aggressor/terrorist) specifically the “mens rea” and “the actus rea” of the crime when there is no laws against of terrorism based on using technology as a tools? However, before discussing deeply, I would like to define the meaning of terrorism in order to connect to the meaning of cyber terrorism.

ANALYSIS

The Meaning of Terrorism and Cyber Terrorism

To define terrorism is not an easy task. Some scholars are facing some difficulties to define it because of considerable disagreement of definition of terrorism. According to Craig Stapley (2009:15), “a quick review of the literature shows that there is no accepted definition in government or in academia”. Kushner (2003: xxiii) furthermore notes that “there are as many definitions for the word terrorism as there are methods of executing it; the term means different things to different people, and trying to define or classify terrorism to everyone’s satisfaction proves impossible.” Louise Richardson (2003) also stipulates that “the widespread usage of the term terrorism, in many contexts, has rendered the word almost meaningless. Today, it’s only universally understood connotation is so pejorative that even terrorists don’t admit to being terrorists any more. A glance at the current usage reveals child abuse, racism, and gang warfare all incorrectly described as terrorism”.

The difficulties of definition term of terrorism as stated above can be understood both theoretically and practically. Even in the United Nations Security Council Resolution 1373 (2001) does not mention a definition of it. As we know, the SC Resolution 1373 (2001) is one of the pillars of the global international work for the prevention and suppression of terrorism (Walter Gehr, 2004: 101-101). It is a non-binding upon member states of the UN resolutions. Its position then plays an important role to fight against the terrorism.

However, difficulties to define it, it does not mean that we have to define it based on what they want to define as terrorism. A clear definition of terrorism has to be tried to be defined because of some essential reasons such as “in any systematic study of a phenomenon, it is necessary to have discrete definitions of the items being studied in order to ensure consistent and valid conclusions. It is especially important to have a concrete definition when there is no clear consensus as to what is and is not terrorism” (Craig Stapley, 2009: 15).

Some definition can be traced in some literature to see various meaning of terrorism. Terrorism can be defined as “the threat or the act of politically violence directed primarily against civilian” Graeme C.S. Steven and Rohan Gunaratna, 2004:7). CIA also has its own definition concerning terrorism, it defines terrorism as “the threat or use of violence for political purposes by individuals or groups, whether action for, or in opinion to established governmental authority, when such actions are intended to shock or intimidate at target group
wider than the immediate victims” (Bambang Abimanyu, 2005:130).

FBI itself states terrorism as “the unlawful use of force or violence against persons or property to intimidate or coerce government, civilization populations, or any segment threat, in furtherance of political or social objective (Bambang Abimanyu, 2005:130). US Army Operational Concept for Terrorism Counteraction notes that terrorism constitutes “the calculated use of violence or threat of violence to attaining goals that are political, religious, or ideological in nature... through intimidate, coercion, or instilling fear” (Bambang Abimanyu, 2005:131).


Those terrorism definition as defined previously has connection to meaning of cyber terrorism. The basic concept of terrorism basically does not change but it has added some elements of crime, as result of using of technologies as the terrorist tool. According to Jason Andress, et.al (2011: 198-199), cyber terrorism is “a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda”.

Similarly to Andress, R. Ahmad and Z. Yunos (2012:149), indicates that cyber terrorism has several attributes such as motivation, impact, and target. R. Ahmad, et.al (2012:232) furthermore explains that term motivation means political, ideological and social; Impact itself refers to mass destruction or seriously interfere critical services operation, cause fear, death or bodily injury, and severe economic loss; and, target is driven to critical national infrastructure computer system and civilian population.

In terms of definition or meaning of terrorism and cyber terrorism as explained above, it can be concluded that there is similarity both meaning of them in some crucial elements such as violence, creating fear, and its target civilian. If in the past, cyber terrorism had been thought as threat in future as mentioned by Andrew Rathmell (1997 : 140), so less than 10 year after his question, cyber terrorism is being a fact and it cannot be wished away. Corporations, government, and private citizen are all at risk and equally all are responsible for preventing and fighting such attacks (Albert J. Marcella, 2000:: 10). All possibilities risks is producing fear in people daily life. It is because people tend to be afraid to something they do not see (invisible) and they do not understand (Ananda Mitra, 2010:55), (Michael Stohl, 2006:225).
Actus Reus and Mens Rea of Cyber Terrorism

To decide elements crime of cyber terrorism basically refers to definition of cyber terrorism. Even though, there is no clear definition of it that has been agreed, it is very important to see element of terrorism as noted in to Security Council Resolution 1371 (2001) concerning Anti-terrorism Resolution and Security Council Resolution 1566 (2004) concerning threats to international peace and security caused by terrorism. The explaining elements of crime of terrorism can be used because of function of the Security Council Resolution is legally binding for UN members. For the purposes of this analysis therefore, I quote those elements as elements crime of cyber terrorism because in "reaffirming of that Resolution stated that "terrorism in all its forms and manifestations constitutes one of the most serious threat to peace and security". It is also because in Paragraph 3 point (a) S. C. Res. 1371 (2001) stated "...intensifying and accelerating the exchange of operational information, especially regarding actions or movements of terrorist persons or networks, and the use of communication technologies againstposite groups...",

Actus reus theoretically consists of three elements. Actus reus refers to the conduct whether he/she has committed. Mens rea is commonly referred to as a subjective element of crime. Mens rea, the mental element or intent of perpetrator to commit crime, can be formed in terms of intention or neglect. Mens rea is called as a subjective element of crime.

Actus reus of cyber terrorism refers to the Security Council Resolution 1373 (2001) in Paragraph 3, as followings: 1. To exchange operational information especially regarding actions or movements of terrorist persons or networks; 2. To forge or falsify travel documents; 3. To traffic in arms; 4. To use explosives or sensitive materials; and 5. To use communication technologies.

Paragraph 3 to the Security Council Resolution 1566 (2004) stated furthermore actus reus of it, as followings (Walter Gehr, 2004: 104): 1. To cause death or serious bodily injury or taking hostages; 2. To provoke a state off error in the general public or in group persons or particular person; 3. To intimidate a population; 4. To compel a government or an international organization to do or to abstain... which constitutes offence within the scope of and as defined... relating to terrorism...."

Both S.C. Res actually had covered element of crime of cyber terrorism (actus reus) indirectly. However, to complete actus reus of cyber terrorism is necessary to put "the use of computers and telecommunications capabilities" as an important element to convergence between cyberspace and terrorism.

The crime also requires criminal intent to be classified as crime. Related to it, mens rea of cyber terrorism is put into intention and knowledge of the perpetrator (terrorist). Intent of the perpetrator (terrorist) means that they have motive in political, social or religious in nature.(Dean Alexander, 2012:70) Whereas knowledge means that they know how to do terror and the effect is coming from the terror in which they generally do not care about their victims.

One of the forms of knowledge of the perpetrators can be found in purpose of the terror. The perpetrators generally realize that what they do (terror) will create fear as noted also in traditional modus of terrorism (P. Flemming and Michael Stohl, 2001:70). In terms of fear, cyber terrorism conveys two significant modern fears: the fear of technology and the fear of terrorism. Both the fear of technology and the fear of terrorism are possible and difficult to be understood. They can create cyber fear that is generated by the fear that what a computer/internet attack can bring down airliners, ruin critical infrastructure, destroy the stock market, reveal nuclear planning secret, etc.

T.L. Thomas,2007

Prosecution of Cyber Aggressors (the Perpetrators/Terrorists)

Prosecution of cyber terrorism will be governed under the same regulation to prosecution of terrorism. Even though there is no exacty definition that is agreed by all states worldwide and scholars/experts, it can be used interpretation to cover cyber terrorism. Pursuant to Article 31 of Vienna Convention 1969, "a treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to terms of the treaty in their context and in the light of its object and purpose".

According to Rebecca M.M. Wallace (1992:228-229), there are 3 (three) main approaches in international law to treaty interpretation. First, the objective approach - interpretation in accordance with the ordinary use of the words of the treaty; Second, the
subjective approach - interpretation in accordance with the intention of the parties to the treaty; and third, the teleological approach - interpretation in accordance with treaty’s aims and objectives.

Those approaches as noted by Wallace can be applied to interpret actus reus and mens rea terrorism to cyber-terrorism as mentioned above. Article 31 of Vienna Convention 1969 furthermore is deemed as “an umbrella law” for covering cyber terrorism, particular in some resolution as indicated in S.C.Res. 1373 (2001), S.C.Res. 1534 (2004), S.C.Res. 1566 (2004) and other S.C.Res. governing terrorism or related to terrorism. They generally oblige to “a state” to counter terrorism in all aspects and issues. The meaning obligation of counter terrorism to “state” is all state shall take control for all terrorism activities in its territory either conducted by a person, a group, or a state. It is therefore that it is pivotal for all countries to have their own laws to deal with terrorism issues, including dealing with law enforcement to the perpetrators (the terrorists).

The terrorism’s perpetrator must be prosecuted not only based on State law but also based on national law of the state. In Indonesia, its regulation of counter terrorism is regulated in Anti-Terrorism Law No. 15 year 2003 concerning the implementation of a Government Regulation in Ministry of Law on Terrorism (Number 1/2002), become the Law. Anti Terrorism Law authorized security officers to arrest and question terror suspects based on intelligence information, detain suspects based on sufficient evidence, close the bank account held by the suspects, open personal mail/documents and tap telephone/communication lines.

In terms of prosecution of the perpetrator, it is governing under article 25 of the Law No. 15 year 2003. The article of the Law No. 15 year 2003 basically governs all perpetrators’ (terrorists) conduct as if mentioned in actus reus and mens rea above, including cyber-terrorism. This regulation was applied for the first time to track down the perpetrators (terrorists) of Bali bombing and then it was adopted as a law for all terrorism cases.

In Unites States itself, regulation of use internet can be seen in the first federal computer crime statute was the Computer Fraud and Abuse Act of 1984 (CFAA). The CFAA is the most important computer crime statute in the US because almost every other statute that deals with computer crime modifies the CFAA. The CFAA makes many acts that are associated with cyber-terrorism prosecutable under US Law. While it does not address the more technical side of cyber-terrorism such as DDoS Attacks, it does address data theft, which, if carried out under the right motives can be associated with cyber terrorism. Also, under Section 1030(a)(2) and (7), the financing of terrorism could possibly be prosecuted under this act (Maxim May, 2004:2).

There is also Federalist No. 10 that agrees not only to the internet’s use but also can be significant assistance to the US campaign against transnational terrorism (Dawinder S. Sidhu, 2010: 3-5). The Federalist mentions that online and mobile media are becoming an integral and part of everyday lives in which computer plays a significant role in data storage and plenty of sensitive personal and institutional information is stored as digital data, particular for national security data. One of cyber terror was at first suspected in the 2003 Northeast blackout, even though it did not attack US Military capabilities and US economy. Other examples of imminent terrorist attacks via the internet can be found in “Electronic Pearl Harbor” or “Digital Waterloo.”

In India, there is India’s Information Technology Act (I.T.A.) of 2000 that addresses the illegal use of the Internet and enables the government of India to prosecute against offences that are associated with cyber terrorism including DDoS attacks. The I.T.A. of 2000 takes into account the understanding that the right to privacy is a part of the right to life and personal liberty enshrined under Article 21 of the Constitution of India The Indian Cyber Crimes Legislation also deals specifically with cyber attacks or recent legislation from the U.S. House of Representatives dealing specifically with cyber terrorism Praveen Dalal, 2006).

Those national regulations of counter terrorism as mentioned above are purposed to prosecute the perpetrators. This is because without punishment, it is difficult to diminish terror including cyber terror or to fight against cyber terrorism.

CONCLUSION

It can be concluded that cyber terrorism is present threat. It has some elements to be fulfilled in order to be categorized as a crime of cyber terrorism. Those elements are qualified as actus reus and mens rea of cyber terrorism.
Both actus reus and mens rea require unlawful means as method of action; network warfare and psychological operation as tools of attack; political, ideological, social and cultural as motivation; critical national infrastructure computer system and civilian population as targets; mass disruption or seriously interfere critical services operation, cause fear, death or bodily injury, and severe economic loss as impact negatively, and cyberspace as domain.

When both actus reus and mens rea are fulfilled, the perpetrators (terrorists) can be prosecuted either applying international law instrument as if Security Council Resolution or national law of states like the Law No. 15 year 2003 concerning Enacting of a Government Regulation in lieu of Law on Terrorism Number 1/2002, some laws in US and India.

REFERENCES


