ANALISIS STRATEGI DALAM MENGHADAPI TOC, KEJAHATAN SIBER, DAN TERORISME DI FILIPINA

STRATEGIC ANALYSIS OF TACKLING THE TOC, CYBER CRIME, AND TERRORISM IN THE PHILIPPINES

Daniel Joko Prasetyo[1]

Universitas Pertahanan

Abstrak - Kejahatan Terorganisir Transnasional (TOC), Kejahatan Siber dan Terorisme adalah ancaman serius bagi banyak negara, terutama negara-negara yang masih lemah dan rawan konflik karena akan menghambat kemajuan negara dan menyebabkan kesenjangan antara masyarakat dan pemerintah, terutama karena akan membawa banyak pelanggaran hukum. Salah satu negara yang bisa dibilang masih lemah dan rentan terhadap konflik adalah Filipina, Filipina menjadi surga bagi para pelaku TOC mengingat lemahnya hukum dan pemerintah negara itu. kasino sangat populer di Filipina sehingga bisnis kasino sangat menguntungkan di negara itu, terutama di masa sekarang banyak kasino menjalankan online untuk memberikan penggemar kasino kemudahan bermain, tetapi juga yang hadir resiko yang besar yang dihadapi saja, seperti penipuan dan hukum pelanggaran. Selain TOC di Filipina sangat marak terjadi kejahatan di dunia maya, banyak terjadi bullying, cyber pornografi, cyber sex dan adanya kelompok teroris Abu Sayyaf Group yang sampai sekarang masih aktif.
Kata kunci: TOC, Cyber Crime, Terrorism, Abu Sayyaf Group

Abstract *- Transnational Organized Crime (TOC), Siber crime and terrorism is a serious threat to many countries, especially countries that are still weak and prone to conflict because it will hinder the progress of the country and led to a gap between the public and the government, mainly because it will bring a lot of lawlessness. One country that arguably still weak and prone to conflict are the Philippines, the Philippines became a haven for the perpetrators of TOC given the weakness of the law and the country's government. casinos are very popular in the Philippines so that the casino business is very profitable in the country, especially in the present lot of casinos to run online casino enthusiasts to provide ease of play, but also present major risks facing it, such as fraud and violations of the law. In addition to the TOC in the Philippines are very rampant crime in cyberspace, a lot going on bullying, cyber pornography, cyber sex and the presence of the terrorist group Abu Sayyaf Group, which is still active.*
Keywords*: TOC, Cyber Crime, Terrorism, Abu Sayyaf Group*

[1] Penulis adalah Mahasiswa Pasca Sarjana Program Studi Peperangan Asimetris Cohort-4 TA. 2016 Fakultas Strategi Pertahanan, Universitas Pertahanan. Penulis dapat dihubungi melalui *email penulis.*

Pendahuluan

Globalisasi yang mewarnai kehidupan masyarakat dunia dewasa ini pada dasarnya adalah fasilitator utama dari berbagai tindak kejahatan/kriminal transnasional, dan sudah meningkat dan bahkan terjadi di dunia maya, dan sekarang ini sudah terkait dengan isu terorisme. Meskipun dalam berbagai literatur, konsepsi kejahatan/kriminal dipisahkan dengan konsepsi terorisme namun dalam tulisan ini akan dijabarkan penelaahan yang lebih mendalam mengenai sinergi antara kedua konsep di atas dan menunjukkan dengan beberapa kasus bahwa terorisme adalah bentuk nyata dari *Transnational Organized Crime* (TOC) yang merupakan produk langsung dari praktek-praktek globalisasi.

Dewasa ini dunia seakan tanpa batas karena manusia dan barang dapat bergerak dengan mudahnya dari negara yang satu ke negara yang lain. Informasi maupun keadaan yang tengah terjadi di suatu negara pun dapat diakses dengan gampang oleh masyarakat yang hidup di negara berbeda. Masyarakat tidak hanya menjadi bagian dari komunitas suatu negara melainkan juga telah menjadi warga negara internasional yang hidup di perkampungan global. Kondisi inilah yang kemudian dikenal sebagai globalisasi. Secara umum, globalisasi merupakan suatu proses terus menerus, di mana terjadi interkoneksitas dari berbagai bidang yang membuat dunia ini menjadi sebuah tempat tunggal yang dihuni oleh masyarakat dunia.

Kemajuan teknologi dan informasi yang dicapai saat ini menciptakan suatuketergantungan terhadap teknologi itu sendiri dalam segala aspek kehidupan terutama yang bersentuhan langsung dengan masyarakat umum seperti sistem transportasi, perbankan, administrasi, entertainment dan lainnya. Di negara-negara maju pada khususnya dimana semua public service menggunakan sistem komputer menjadikan teknologi ini sebagai suatu hal yang sangat virtal, kondisi ini dapat dilihat seperti di Jepang, Amerika Serikat, Inggris, Perancis, dan negara-negara maju lainnya. Internet membuat suatu fenomena dunia global dimana terbentuknya suatu komunitas dunia dengan tidak membatasi latar belakang darisetiap penggunanya, tidak terbatas pada usia anak tertentu, dewasa hingga lansia, berbagai status sosial, bangsa dan ras mana saja.

Internet adalah produk dari globalisasi yang telah menciptakan dunia baru yang disebut dengan *cyber space* yaitu dunia komunikasi yang berbasis

komputer yang menawarkan realitas yang baru yang berbentuk virtual (tidak langsung dan tidak nyata). Walaupun demikian, dikatakan virtual, internet membuat globe dunia, menjadikan dunia semakin menyatu. Kita dapat merasakannya, seolah-olah berada pada tempat tersebut dan melakukan hal-hal yang nyata seperti bertransaksi dan berdiskusi. Secara etimologis, istilah cyber space sebagai suatu kata merupakan suatu istilah baru yang hanya dapat ditemukan di dalam kamus mutakhir. Cambridge Advanced Learner'sDictionary memberikan definisi cyberspace sebagai "*the Internet considered as an imaginaryarea without limits where you can meet people and discover information about any subject*". *The American Heritage Dictionary of English Language Fourth Edition* mendefinisikan *cyberspace* sebagai "*the electronic medium of computer networks, in which onlinecommunication takes place*".

TOC merupakan sebuah kejahatan terorganisir yang kontrol dan manajemennya bersifat lintas batas negara, dengan kata lain TOC merupakan kejahatan terorganisir yang melibatkan sedikitnya dua negara. Secara global, TOC merupakan sebuah ancaman yang dianggap serius oleh negara-negara baik negara maju, berkembang, maupun negara miskin, hal ini terbukti dengan terlaksananya konvensi perlawanan terhadap kejahatan transnasional terorganisasi (*Convention against Transnational Organized Crime*) oleh PBB.

Penanganan kasus TOC bagi negara-negara maju seperti Amerika Serikat dan Inggris tentunya akan lebih mudah dilakukan melihat kemampuan yang pemerintah mereka miliki tentunya akan sangat membantu memberantas jaringan TOC di negara-negara tersebut. Namun permasalahannya adalah bagaimana jika TOC memiliki basis di negara yang lemah dan rentan terhadap konflik, tentunya hal ini memunculkan sebuah tantangan tersendiri bagi negara tersebut dimana pemerintah memiliki double desk bagi negaranya yaitu untuk mempertahankan kestabilan negara terhadap ancaman konflik yang bisa terjadi kapanpun dan untuk memberantas jaringan TOC yang bercokol di negaranya.

Ada alasan tertentu mengapa TOC memilih negara lemah sebagai basis dari kegiatannya, antara lain adalah:

1. Negara lemah berarti pemerintahnya pun lemah
2. Banyak masyarakat awam yang bisa dimanfaatkan dalam kegiatannya

3. Banyak kelompok yang bisa diajak kerjasama.

Pertama, negara lemah biasanya dikarenakan pemerintahnya yang lemah dimana banyak masalah yang tidak bisa diselesaikan pemerintah, korupsi, dan hilangnya Kepercayaan masyarakat kepada pemerintah merupakan celah-celah yang sangat menguntungkan bagi TOC, terutama masalah korupsi dimana tentunya akan sangat mudah bagi TOC untuk merekrut para birokrat untuk bergabung dan melindungi kegiatan TOC hanya dengan memberinya secuil dari sekian banyak keuntungan yang dimiliki TOC. Kedua, komposisi negara lemah tentunya lebih banyak didominasi oleh masyarakat awam yang notabenenya sangat mudah dibutakan oleh TOC, dimanfaatkan untuk kegiatannya, dan pada akhirnya dijadikan kambing hitam jika kegiatan TOC tersebut terancam. Terakhir adalah di negara lemah banyak terdapat kelompok-kelompok penjahat yang dapat dimanfaatkan keberadaannya oleh TOC untuk mendukung kegiatan kejahatannya, kelompok penjahat ini juga menjadi salah satu penyebab negara-negara lemah sering dilanda konflik.

Kebanyakan merupakan warga negara asing yang mengoperasikan kegiatannya di Filipina Contoh kasus yang akan diangkat penulis adalah kasus TOC, Cyber Crime yang banyak terjadi di Filipina yang merupakan salah satu negara fragile atau rapuh, Filipina telah menjadi salah satu surga bagi para pelaku tindak kejahatan TOC dan Cyber Crime termasuk kedalamnya pornografi maya, sarang seks online, judi online illegal, penipuan kartu kredit, dan pencurian identitas. Banyak TOC yang memanfaatkan kelemahan pemerintah Filipina terutama karena ketidakmampuan organisasi dan tehnik pemerintah dalam upaya memberantas kejahatan maya (*cyber-crime*). Lebih jauh lagi, menurut

Badan Investigasi Kriminal dan kelompok deteksi Filipina (CIDG), dari sekian banyak kegiatan TOC yang terjadi, pelaku.

Definisi strategi, TOC, Cyber Crime dan Terrorism

Menurut Anthony, Parrewe dan Kacmar (1999) strategi dapat didefinisikan sebagai formulasi misi dan tujuan organisasi, termasuk di dalamnya adalah rencana aksi (action plans) untuk mencapai tujuan tersebut dengan secara eksplisit mempertimbangkan kondisi persaingan dan pengaruh-pengaruh kekuatan di luar organisasi yang secara langsung atau tidak berpengaruh

terhadap kelangsungan organisasi (Nainggolan, 2008)

Transnasional Organized Crimes (TOC) adalah salah satu kejahatan terorganisir dalam cangkupan internasional atau melibatkan banyak negara. TOC ini sama halnya dengan sebuah organisasi internasional, namun TOC ini lebih bertujuan melakukan hal-hal ilegal seperti terorisme, perdagangan manusia, dan lain sebagainya. TOC memiliki sistem khusus dalam menjalankan misi dan visi mereka. Dalam menjalankan misi mereka dapat melakukan kekerasan dan dilakukan dengan sistematis yang sudah ditentu.

TOC ini pun menjadi sulit di selesaikan karena ini mencangkup banyak negara dan mereka saling berhubungan tidak ada tindakan yang tidak diketahui, mereka menggunakan berbagai cara agar sulit diketahui oleh negara, mereka terus berkembang di setiap negara. Mereka membuat aliansi dan bekerjasama dalam melakukan kejahatan negara. Ada 6 Karakteristik kejahatan transnasional berdasarkan pertemuan Internasional *The World Ministerial Conference on Organized Crime* di Nepal pada tahun 1994, yaitu:

1. Suatu organisasi yang melakukan kejahatan (*group organization to commit crime*)
2. Memiliki jaringan hirarkis atau hubunga personel yang memberikam kewenangan pemmpinnya untuk mengendalikan kelompok tersebut (*hierarcical links or personal relationship which permit leader to control the group*)
3. Kekerasan, intimidasi, dan korupsi digunakan untuk mendapatkan keuntungan atau mengontrol daerah kekuasaan atau pasar (*violence, intimidation, and coruption used to earn profit or control teritories or markets*)
4. Mencuci uang hasil perdagangan gelap baik yang berasal dari kegiatan kriminal dan disusupkan dalam kegiatan ekonomi yang sah (*laundring of illicit process both in furtherence of criminal activity and to infiltrate in legitimacy economy*)
5. Memperluas jaringan operasinya keluar negeri (*the potential for expansion into any new activities and beyond national borders*
6. Bekerjasama dengan kelompok kejahatan transnasional terorganisir lainnya (*cooperation with other organized transnational criminal group*).

Gambar 1 *Organisasi crime di Dunia*[1]

Beberapa pendapat mengenai *cyber crime*. Menurut Gregory (2005) *Cybercrime* adalah suatu bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung ke internet, dan mengekploitasi komputer lain yang terhubung dengan internet juga. Adanya lubang-lubang keamanan pada sistem operasi menyebabkan kelemahan dan terbukanya lubang yang dapat digunakan para *hacker*, *cracker* dan *script kiddies* untuk menyusup ke dalam computer tersebut, sedangkan menurut Tavani (Fajri, 2008) definisi *Cybercrime*, yaitu "kejahatan dimana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi *cyber* dan terjadi di dunia *cyber*".

Modus Operasi *cyber crime*

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operasi yang ada antara lain (Golose, 2006) :

a. *Unauthorized Access to Computer System and Service*

b. *Illegal Contents*
c. *Data Forgery*
d. *Cyber Espionage*
e. *Cyber Sabotage and Extortion*
f. *Offense against Intellectual Property*
g. *Infringements of Privacy*

Secara umum istilah terorisme diartikan sebagai bentuk serangan (faham/ideologi) terkoordinasi yang dilancarkan oleh kelompok tertentu dengan maksud untuk membangkitkan perasaan takut di kalangan masyarakat. Gerakan ini sering menggunakan teknik bom bunuh diri yang dilakukan oleh anggota kelompoknya secara sukarela.

Dr. F. Budi Hardiman dalam artikelnya yang berjudul "Terorisme: Paradigma dan Definisi" menyatakan bahwa "Terorisme merupakan kegiatan yang sudah cukup tua dalam sejarah umat manusia. Fenomena menakut-nakuti, mengancam, memberi kejutan kekerasan atau membunuh dengan maksud menyebarkan rasa takut adalah taktik-taktik yang sudah melekat dalam perjuangan kekuasaan, jauh sebelum hal-hal itu dinamai terror atau terorisme".

Tulisan ini diharapkan dapat memberikan manfaat yang berguna bagi masyarakat terlebih untuk bangsa Indonesia dalam menghadapi TOC, Indonesia dapat merencanakan dan membuat strategi dalam menghadapi TOC, Cyber Crime bahkan untuk menanggulangi terorisme yang masih marak terjadi.

Tulisan ini akan menggunakan metode kualitatif dalam penulisan makalah. Metode ini dilakukan dalam memperoleh data-data yang diperlukan melalui studi literatur, studi pustaka serta *online research*. Basis dari penelitian ini adalah data sekunder yang diperoleh dari berbagai sumber informasi yang relevan mengenai strategi antara institusi publik dan institusi militer baik dalam menghadapi TOC, cyber crime dan terorisme, di samping penggunaan landasan teoritis pendukung lain yang relevan.

Transnasional organized crime, cyber crime, terrorism di Filipina

TOC merupakan sebuah kejahatan terorganisir yang kontrol dan manajemennya bersifat lintas batas negara, dengan kata lain TOC merupakan kejahatan terorganisir yang melibatkan sedikitnya dua negara. Secara global, TOC merupakan sebuah ancaman yang dianggap serius oleh negara-negara baik negara maju, berkembang, maupun negara miskin dan TOC rentan memasuki negara – negara yang rentan terhadap konflik dan negara yang lemah, hal ini

terbukti dengan terlaksananya konvensi perlawanan terhadap kejahatan transnasional terorganisasi (*Convention against Transnational Organized Crime*) oleh PBB.

Kasus TOC yang banyak terjadi di Filipina yang merupakan salah satu negara fragile atau rapuh, Filipina telah menjadi salah satu surga bagi para pelaku tindak kejahatan TOC termasuk kedalamnya *cyber crime* (pornografi maya, sarang seks online, judi online illegal, penipuan kartu kredit, dan pencurian identitas). Banyak TOC yang memanfaatkan kelemahan pemerintah Filipina terutama karena ketidakmampuan organisasi dan tehnik pemerintah dalam upaya memberantas kejahatan maya (cyber-crime). Lebih jauh lagi, menurut Badan Investigasi Kriminal dan kelompok deteksi Filipina (CIDG), dari sekian banyak kegiatan TOC yang terjadi, pelaku kebanyakan merupakan warga negara asing yang mengoperasikan kegiatannya di Filipina.

Salah satu pelaku TOC yang beroperasi di Filipina adalah kelompok Shin Un-Sun, Shin sendiri merupakan warga negara Korea Selatan yang melakukan TOC di Filipina yang bergerak pada bidang *cyber-crime*, dia sendiri merupakan orang yang diburu di Filipina dan Korea Selatan karena beberapa penipuan internet skala besar, antara lain membajak server telekomunikasi terbesar di Filipina, bursa efek Korea, dan membajak databank perusahaan Hyundai Capital Corp. Dalam proses investigasi, Shin mengaku bahwa dia pergi ke Filipina untuk mengembangkan program kasino online ilegal yang menjadi pendapatan utama para mafia selama bertahan-tahun. Shin juga menyatakan bahwa mafia Korea sering menjadikan orang-orang Filipina sebagai target operasi pencucian uang dan penipuan kartu kredit transnasional.

Dari contoh kasus diatas, dapat dianalisis bahwa Shin yang merupakan warga negara Korea yang melakukan TOC di Filipina memiliki alasan tertentu mengapa kelompoknya membidik Filipina sebagai lahan untuk menjalankan operasi TOC di bidang *cyber-crime*. Berdasarkan tulisan sebelumnya ada tiga alasan yang menjadi faktor pendorong, pertama adalah lemahnya pemerintah yang dibuktikan dengan lemahnya pemerintah Filipina dalam hal organisasi dan teknik dalam upaya pemberantasan cyber-crime, kedua adalah banyak masyarakat awam yang bisa dimanfaatkan untuk kegiatannya, hal ini dibuktikan dengan pernyataan Shin yang mengatakan bahwa banyak mafia-mafia Korea memanfaatkan

orang Filipina untuk menjadi target pencucian uang dan penipuan kartu kredit, dan ketiga adalah banyak kelompok yang bisa diajak bekerjasama, dalam hal ini kelompok Shin menjalankan usaha kasino online ilegal di Filipina, banyaknya kerjasama yang dibangun Shin terbukti dengan banyaknya kasino di Filipina yang menjalankan program kasino online ilegal milik Shin, menurut laporan setidaknya ada tujuh kasino yang sudah diperiksa polisi Filipina terkait dengan kasino online ilegal tersebut.

TOC yang terjadi disebabkan oleh lemahnya struktural yang ada di Filipina, kelemahan struktural ini bisa disebabkan oleh beberapa hal, antara lain memang negara tersebut lahir lemah, tidak mampu mengontrol teritori atau kawasan, pengurangan bantuan luar negeri, dan maraknya korupsi, ketidakcakapan administrasi, dan ketidakmampuan mempromosikan pembangunan ekonomi. Dalam hal ini Filipina masuk dalam kategori ketidakcakapan administrasi dimana CIDG sendiri sebagai badan negara dalam mengatasi masalah kriminal mengakui bahwa penyebab Filipina menjadi surga bagi para pelaku TOC adalah karena ketidakmampuan pemerintah dalam hal pengorganisasian dan teknik untuk memberantas TOC terutama dalam hal cyber crime.

Selain kelemahan struktural pemerintah Filipina, hal yang paling menjadi permasalahan adalah bahwa judi merupakan suatu yang popular di negara Lumbung Padi tersebut, banyak orang kaya yang menggunakan uangnya untuk pergi ke kasino ataupun membuka situs kasino *online*, bertaruh, dan menghabiskan waktu luang untuk berjudi. Permasalahan baru tentunya akan muncul dimana ada peraturan pemerintah yang menetapkan bahwa minimal umur untuk bermain kasino online di Filipina adalah umur 21 dan banyak anak dibawah umur tersebut yang berusaha secara diam-diam bermain kasino *online*, dan ketika kasino *online ilegal* yang dijalankan kelompok Shin Un-Sun beroperasi di Filipina, maka tentunya akan sangat mudah bagi pengguna dibawah umur untuk masuk kedalam pusaran kasino online yang seharusnya tidak diperbolehkan, dan kasino ilegal sangat rentan terhadap penipuan terutama penipuan kartu kredit.

Banyak *cyber crime* yang terjadi di Filipina, Menurut siaran pers dari Kepolisian Nasional *Filipina Anti-Cybercrime Group* (PNP ACG), total 1.211 pengaduan *cybercrime* diajukan dengan mereka 2013-2015. Lima keluhan atas

terima adalah penipuan *online* (366), pencemaran nama baik secara *online* (240), ancaman online (129), pencurian identitas (127), dan foto dan video yang vulgar (89).[2]

Terorisme mungkin merupakan ancaman terbesar bagi keamanan masyarakat di Filipina dan terus menjadi masalah yang meningkat dan berkelanjutan. Wilayah selatan Filipina adalah daerah terlarang antara lain: Wilayah Mindanao, Kepulauan Sulu dan Semenanjung Zamboanga semua dianggap sangat berbahaya. Kelompok teroris Front Pembebasan Islam Moro (MILF) telah disalahkan untuk banyak insiden kekerasan, penculikan, dan bentrokan sering dengan pasukan keamanan Filipina.

***Gambar 2** cyber crime* di Filipina[1]

[2]http://www.gmanetwork.com/news/story/534597/scitech/technology/top-5-cybercrimes\complaints-in-the-philippines-according-to-pnp#sthash.v28hfkjv.dpuf

Kelompok teroris, seperti Abu Sayyaf dan Jama'ah Islamiyah, telah memisahkan diri dari MILF dan sangat berbahaya. Mereka bertanggung jawab atas pemboman yang mengakibatkan kerusakan properti, cedera dan kematian, terlebih saat ini kelompok teroris Abu Sayyaf sedang menyandera beberapa orang dan meminta tebusan sebagai syarat pembebasan para sandera, dan apabila tidak menurutinya, kelompok ini tidak segan – segan membunuh para sandera tersebut, seperti yang sudah dilakukan terhadap warga kanada yang menjadi sandera selama tujuh bulan yang akhirnya dipenggal oleh kelompok teroris tersebut.[3]

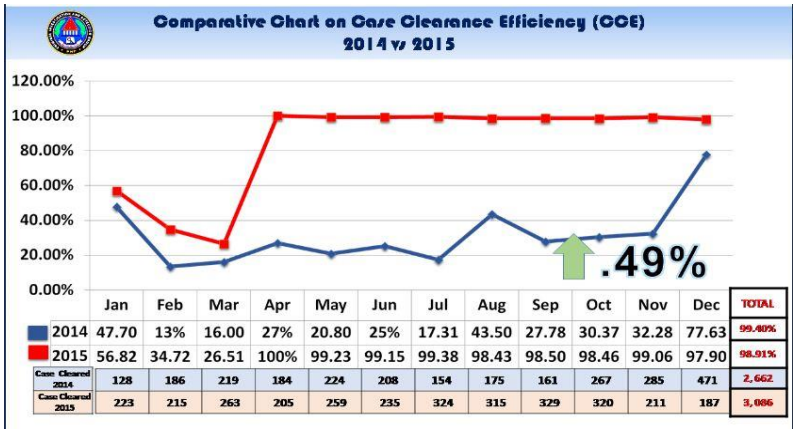
Selama beberapa tahun terakhir, aksi terorisme yang melibatkan bahan peledak terjadi di Utara Cotabato, Basilan, Isabela City, Jolo, Cotabato City, Makati dan bandara Zamboanga telah mengakibatkan kematian 41 orang dan luka parah lebih dari seratus orang. Sebagian besar pemboman ini terjadi pada angkutan umum, seperti bus, dan di lokasi ramai seperti restoran dan katedral.

Pencegahan dan Penanggulangan *Transnasional organized crime, cyber crime, terrorism* di Filipina

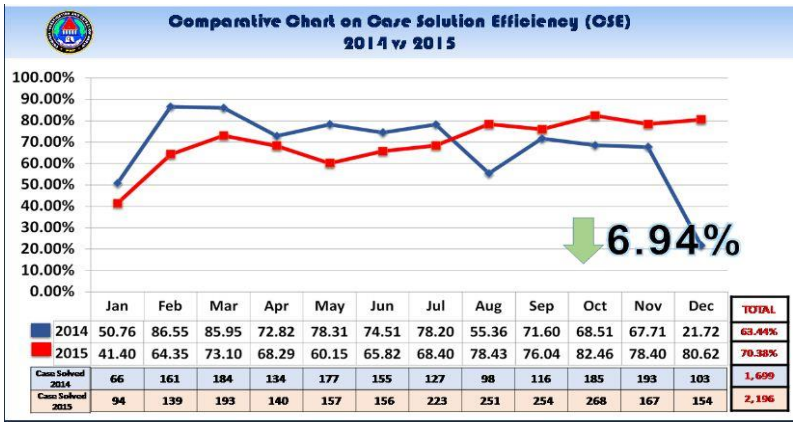
Pemerintah Filipina membentuk suatu Badan Investigasi Kriminal dan kelompok deteksi Filipina (CIDG) untuk memberantas TOC.

Pemerintah Filipina mendukung pengembangan kapabilitas organisasi dan teknik untuk memberantas cyber-crime melalui CIDG. CIDG sendiri telah berhasil menangani masalah TOC yang terjadi. Contohnya kasus Shin Un-Sun, CIDG berhasil menangkap Shin Un-Sun dengan alasan telah melakukan tindak kejahatan maya transnasional karena Shin merupakan warga negara Korea dan melakukan kejahatan maya di Filipina dengan bantuan mafia-mafia yang ada di Korea. Shin tertangkap ketika sedang meretas databank sebuah perusahaan menggunakan laptop pribadinya Komparasi data kejahatan yang sudah diolah oleh CIDG.

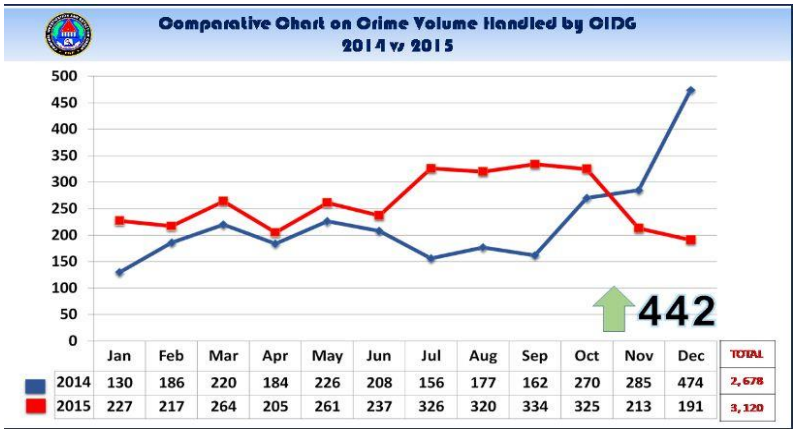
[3]http://internasional.kompas.com/read/2016/04/26/06390861/Tujuh.Bulan.Disandera.Warga.Kanada.Akhirnya.Dipenggal.Abu.Sayyaf



Gambar 3 .Comparative chart on Case Clearance Efficiency (CCE)



Gambar 4 .Comparative chart on Case Solution Efficiency (CSE)



Gambar 5 .Comparative chart on Crime Volume handled by CIDG[4]

[4]http://www.cidg.pnp.gov.ph/page/index.php?option=com_content&view=article&id=174&Itemid=137

Filipina memiliki perlindungan hukum terhadap konsumen yang menggunakan internet dan diatur dalam *Electronic Commerce Act* 2000 dan *Consumer Act* 1991 yang menyebutkan bahwa siapa saja yang menggunakan transaksi secara elektronik tunduk terhadap hukum yang berlaku. Dan Filipina sudah memiliki cyberlaw yang mengatur tentang cyber crime, hak cipta intelektual dan yang satu – satunya di negara ASEAN yang sudah memiliki aturan *Online Dispute resolution* (ODR), ODR adalah resolusi yang mengatur perselisihan di internet yaitu dengan adanya *Philippines Multi Door Courthouse*[5].

Strategi dalam Penanganan Transnasional *organized crime, cyber crime, terrorism* di Filipina

Pemerintah Filipina menjalin kerja sama dengan Indonesia dalam menangani terorisme, karena aksi dari tindakan terorisme yang terjadi di Indonesia dan di Filipina dianggap sebagai tindakan yang dapat mengancam stabilitas kawasan yang terdapat di kedua negara, maupun di kawasan Asia Tenggara dan tindakan terorisme merupakan tindakan kekerasan yang dilakukan secara terorganisir, dapat terjadi dimana dan kapan saja.

Dukungan yang saling diberikan oleh kedua negara membawa kondisi Indonesia dan Filipina menjadi lebih stabil, serta kerjasama yang dilakukan oleh kedua negara berhasil membantu penyelesaian konflik-konflik mengenai isu-isu keamanan yang terdapat di kedua negara.

Selain menjalin kerja sama dengan Indonesia, Filipina juga melakukan kerja sama dengan Amerika dalam menangani teroris Abu Sayyaf Group di bidang militer, Amerika menganggap Abu Sayyaf Group adalah teroris setelah kejadian penculikan terhadap warga Amerika pada tahun 2001, sehingga Amerika juga bersedia bekerja sama dengan Filipina untuk memberantas teroris Abu Sayyaf Group. Filipina juga aktif dalam organisasi ASEAN. Filipina adalah satu dari tiga negara anggota ASEAN yang menandatangani persetujuan anti terorisme (*Agreement on Information Exchange and Establishment of Communication Procedures*) di Manila pada 7 Mei 2002, dalam kerangka kerjasama ini akan mengikut sertakan seluruh lembaga dalam negeri negara masing-masing yang terkait dengan pertahanan keamanan. Pengaitan antara

[5] http://ug-komputer.blogspot.co.id/2014/12/perbandingan-undang-undang-ite-negara.html

terorisme dan ASEAN dicantumkan dalam Special ASEAN Ministerial Meeting on Terrorism yang di keluarkan di Kuala Lumpur pada 21 Mei 2002. Yang dilanjutkan dengan penugasan para pejabat senior masing-masing negara kawasan Asia Tenggara untuk melaksanakan *Work Programme on Terrorism to Implement the ASEAN Plan of Action to Combat Transnational Crime*[6].

Kesimpulan

TOC kasino *online* yang dioperasikan Shin Un-Sun di Filipina memiliki dampak yang buruk bagi warga Filipina terutama karena masalah penipuan kartu kredit dan potensi pelanggaran hukum yang besar, dan masih sering terjadi cyber crime di Filipina, dan menurut siaran pers dari Kepolisian Nasional Filipina *Anti-Cybercrime Group* (PNP ACG), ada 1.211 pengaduan *cyber crime* yang terjadi pada tahun 2013-2015. Ada 5 aduan atau keluhan yang teratas dalam *cyber crime* yaitu:

1. penipuan *online* sebanyak 366
2. pencemaran nama baik secara *online* sebanyak 240
3. ancaman *online* sebanyak 129
4. pencurian identitas sebanyak 127
5. foto dan video yang vulgar sebanyak 89

Selain permasalahan TOC, *Crime Cyber*, Filipina juga menghadapi terorisme yang juga sangat menggangu keamanan negaranya dan yang sampai sekarang masih aktif adalah kelompok teroris Abu Sayyaf Group, yang saat ini juga sedang menyandera Warga Negara Indonesia.

Dalam upaya pencegahan dan penanggulangan TOC, *Cyber Crime dan Terrorism*, Pemerintah Filipina membentuk suatu Badan Investigasi Kriminal dan kelompok deteksi Filipina (CIDG), CIDG ini sudah bekerja dengan baik, CIDG berhasil menangkap Shin Un-Sun salah satu pelaku tindakan TOC yang beroperasi di Filipina, Shin un-Sun adalah warga negara Korea, Pemerintah Filipina juga sudah memiliki perlindungan hukum terhadap konsumen yang menggunakan internet dan diatur dalam *Electronic Commerce Act* 2000 dan *Consumer Act* 1991 yang menyebutkan bahwa siapa saja yang menggunakan transaksi secara elektronik tunduk terhadap hukum yang berlaku. Dan Filipina sudah memiliki cyberlaw yang mengatur tentang cyber crime, hak cipta intelektual dan yang satu – satunya di negara ASEAN yang sudah memiliki aturan *Online Dispute resolution* (ODR), ODR adalah resolusi yang

[6] http://nickycatlovepink.blogspot.co.id/2009/05/pendahuluan-1.html

mengatur perselisihan di internet yaitu dengan adanya Philippines Multi Door Courthouse.

Strategi yang dilakukan Filipina dalam penanggulangan TOC, Cyber Crime dan Terrorism adalah dengan melakukan kerja sama dengan berbagai negara, contohnya negara Amerika, mereka bekerja sama dalam bidang militer untuk pemberantasan teroris Abu Sayyaf Group, selain dengan negara amerika, pemerintah Filipina juga bekerja sama dengan Indonesia dalam penanganan terorisme, bahkan keduanya negara ini sudah membuat MOU dalam menangani terorisme yang terjadi di kedua negara tersebut. Filipina juga aktif di dalam ASEAN.

Indonesia sendiri saat ini juga mengalami permasalahan yang sama dengan Filipina, di Indonesia juga banyak mengalami *cyber crime*, dari pencucian uang, pornografi. dan bahkan di Indonesia Terorisme masih menjadi sesuatu yang serius untuk di tangani, Teroris di Indonesia yang sampai sekarang masih dalam pengejaran adalah kelompok Santoso yang diindikasi berada dalam wilayah Poso, Sulawesi Tengah dan bahkan masih banyak teroris yang lain yang bahkan mereka mendeklarasikan sebagai simpatisan dari ISIS.

Upaya pencegahan terhadap tindakan TOC, cyber crime dan terrorism sudah dilakukan oleh Indonesia, Indonesia memiliki Kementerian Komunikasi dan Informasi untuk menangani TOC, dan cyber crime, bahkan saat ini Indonesia memiliki Badan khusus sendiri untuk menangani masalah cyber yaitu Badan Siber Nasional (BSN) yang berada di bawah LEMSANEG (Lembaga Sandi Negara). Selain itu Indonesia juga memiliki badan khusus yang menanggulangi terorisme yaitu Badan Nasional Penanggulangan Terorisme (BNPT).

Permasalahan TOC, *cyber crime* dan Terorisme yang terjadi di Filipina tidak jauh berbeda dengan yang terjadi di Indonesia, sehingga langkah – langkah dan strategi yang diambil oleh kedua negara hampir sama dan bahkan kedua negara melakukan kerja sama dan membuat MOU khusus untuk menangani terorisme. Kedua negara juga ikut tergabung dalam ASEAN, sehingga koordinasi yang dilakukan oleh kedua negara berjalan dengan baik.

Saran

Beberapa hal yang dapat dijadikan sebagai saran dengan hasil penelitian diatas adalah:

1. Pemerintah Filipina dan Indonesia lebih sering berkomunikasi dan bekerja sama dalam hal keamanan di kedua negara tersebut.

2. Undang – Undang mengenai TOC, Cyber crime dan terrorism semakin diperjelas, sehingga lebih jelas penegakan hukum bagi yang melanggarnya.

3. Perlu adanya hukum yang spesifik atau khusus yang berkaitan dengan TOC, *cyber crime* dan terorisme karena tindakan TOC, *Cyber crime* dan terorisme sangat berbahaya dan merugikan banyak pihak.

Daftar Pustaka

Artikel Buku

Golose, Petrus Reinhard, 2006, "Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia oleh Polri", Buletin Hukum Perbankan dan Kebanksentralan Vol.4 Nomor.2 Agustus 2006

Artikel Jurnal

Fajri, Anthony, April 2008,"Cybercrime" http://students.ee.itb.ac.id/fajri/publication.

Artikel *Online*

Gregory, Thomas HA, 2005 "Ketenaran Cybercrime di Indonesia", Makalah STIMIK Perbanas 2005 yang dipublikasikan diakses pada 16 Juli 2016.

Artikel Lainnya

http://www.gmanetwork.com/news/story/534597/scitech/technology/top-5-cybercrimes-complaints-in-the-philippines-according-to-pnp#sthash.v28hfkjv.dpuf

http://internasional.kompas.com/read/2016/04/26/06390861/Tujuh.Bulan.Disandera.Warga.Kanada.Akhirnya.Dipenggal.Abu.Sayyaf

http://geometrx.com/wp-content/uploads/2011/02/Organized-Crime-Map.png (gmabr crime)

http://marsyaholmes.blogspot.co.id/2014/06/transnational-organized-crime-toc.html

http://www.gmanetwork.com/news/story/534597/scitech/technology/top-5-cybercrimes-complaints-in-the-philippines-according-to-pnp

http://www.acg.pnp.gov.ph/

https://www.worldnomads.com/travel-safety/southeast-asia/philippines/areas-to-avoid-in-the-philippines

http://www.cidg.pnp.gov.ph/page/index.php

http://www.napolcom.gov.ph/

http://www.dilg.gov.ph/

http://www.cidg.pnp.gov.ph/page/index.php?option=com_content&view=article&id=174&Itemid=137

http://ug-komputer.blogspot.co.id/2014/12/perbandingan-undang-undang-ite-negara.html

http://gopego.com/news/a/2012/10/ditentang-banyak-pihak-pemerintah-filipina-tangguhkan-uu-cybercrime

http://www.beritasatu.com/nasional/9131-indonesiafilipina-perangi-terorisme.html