Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance
p-ISSN: 2797-9598 | e-ISSN: 2777-0621
Vol. 5 No. 2 Mei- Agustus 2025

SERANGAN *MALWARE RANSOMWARE* DALAM PERSPEKTIF *TRANSNATIONAL CRIME*

Dewi Pika Lbn Batu[1], Parlaungan Gabriel Siahaan[2], Taufiq Ramadhan[3], Agnes Irene Silitonga [4]
[1,2,3]Fakultas Ilmu Sosial, [4]Fakultas Ekonomi Universitas Negeri Medan
Email: [1]dewi_pika_lumban@unimed.ac.id, [2]parlaungansiahaan@unimed.ac.id, [3]TaufiqRamadhan@unimed.ac.id, [4]agnesirenesilitonga@unimed.ac.id

Abstract

Nowadays, malware attacks are a national and global concern. Malware is software designed to harm or disrupt computers in some way including viruses, worms, Trojans, backdoors, ransomware and other malicious programs. Malware spreads and infects computer systems in various ways. In this research, the author focuses on studying ransomware. Ransomware is a form of malware that infiltrates computer devices to block access to information, basically blocking files and demanding ransom to give access back to the information. Hackers use the double extortion method, encrypting and stealing data with the threat of being published to the media if the ransom is not paid immediately. In recent years, ransomware attacks have occurred in Indonesia, such as the wannacry ransomware attack on Harapan Kita Hospital and Dharmais Hospital, the lockbit ransomware attack on Bank Syariah Indonesia and the ramsonware brain cipher attack on the National Data Center. Moreover, cybercrime is a transnational crime, which can be committed across national borders, so in this case regulation is also a major challenge in handling cybercrime cases.
Key words: Malware, Ransomware, Cybercrime, Transnational crime.

Abstrak

Dewasa ini serangan malware menjadi perhatian nasional maupun global. *Malware* merupakan perangkat lunak yang dirancang untuk membahayakan atau mengganggu komputer dengan cara tertentu mencakup *virus, worm, Trojans, backdoors, ransomware* dan program berbahaya lainnya. *Malware* menyebarkan dan menginfeksi sistem komputer dengan berbagai cara. Dalam penelitian ini, penulis fokus untuk mengkaji mengenai *ransomware*. *Ransomware* merupakan bentuk *malware* yang menyusup keperangkat komputer untuk memblokir akses ke informasi, pada dasarnya akan memblokir file dan meminta uang tebusan untuk memberikan akses kembali ke informasi. *Hacker* menggunakan metode *double extortion*, mengenkripsi dan mencuri data dengan ancaman akan di publish ke media apabila tidak segera membayar tebusan. Beberapa tahun terakhir serangan kasus *ransomware* banyak terjadi di Indonesia seperti serangan *ransomware wannacry* di Rumah sakit Harapan Kita dan Rumah Sakit Dharmais, serangan *ransomware lockbit* terhadap Bank Syariah Indonesia dan serangan *ramsonware brain cipher* terhadap Pusat Data Nasional. *Locus delicti* menjadi tantangan penegak hukum dalam menyelidiki kasus *cybercrime ransomware*. Selain itu, *cybercrime* merupakan termasuk kejahatan *transnational crime*, yang dapat dilakukan antar lintas batas negara, sehingga dalam hal ini regulasi juga menjadi tantangan utama dalam penanganan kasus *cybercrime*.
Kata kunci: *Malware, Ransomware, Cybercrime, Transnational crime.*

PENDAHULUAN

Kemajuan teknologi telah mempengaruhi peradaban manusia. Kemajuan teknologi dapat dirasakan dalam berbagai bidang, seperti: ideologi, politik, ekonomi, sosial dan budaya, pertahanan dan keamanan, Pendidikan, kesehatan, hiburan, dan bidang lainnya. Teknologi informasi dan media elektronik dinilai sebagai simbol pelopor, yang akan mengintegrasikan seluruh sistem dunia, baik

dalam aspek sosial, budaya, ekonomi, dan keuangan. Namun, tidak dapat diindahkan bahwa segala sesuatu hasil ciptaan manusia akan selalu memberikan dampak negatif, hal ini terjadi karena penyalahgunaan ataupun ketidakpuasan manusia untuk terus maju dan berkembang meskipun dengan cara yang tidak sepatutnya atau illegal. Akibatnya muncul berbagai fenomena kejahatan-kejahatan baru yang dilakukan melalui perantara komputer dan/atau pemanfaatan jaringan internet yang disebut dengan kejahatan dunia maya atau *cybercrime*.[1]

Istilah lain dari *cybercrime* disebut juga *virtual crime, internet crime, computer fraud, computer related offence, computer crime, online crime*. Dalam Black's Law Dictionary, *cyber crime* didefinisikan *Crime requiring knowledge of computer technology, such as sabotaging or stealing computer data or using a computer to commit some other crime.* Perbedaan *Cyber crime* dan kejahatan konvensional dapat dilihat dari cara melakukannya. Penjahat dunia nyata menggunakan senjata, sedangkan penjahat dunia maya menggunakan teknologi komputer. Kejahatan dunia maya merupakan migrasi kejahatan dunia nyata ke *cyber space*. *Cyber space* menjadi alat yang digunakan untuk melakukan kejahatan lama dengan cara baru.[2]

Populer di era ini, internet sudah menjadi bagian terpenting dalam kehidupan manusia sebagai alat komunikasi, sumber ilmu pengetahuan, sumber informasi dan sumber penghasilan. Indonesia termasuk salah satu negara dengan jumlah pengguna internet yang cukup tinggi. Hal ini membuktikan masyarakat Indonesia terbuka dengan kemajuan teknologi. Menurut perkiraan sampai pada tahun 2018 Indonesia menempati peringkat keenam setelah Jepang pengguna internet terbanyak di seluruh dunia sekitar 123 juta pengguna.[3] Namun, dampak negatif kemajuan teknologi telah merusak norma-norma yang hidup di suatu negara. Kemampuan untuk memasuki suatu negara tanpa batas adalah faktor yang menyebabkan munculnya kejahatan modern, tidak terlepas dari perkembangan teknologi dan informasi yang menjadi bagian dari kehidupan masyarakat modern.[4] Berita hoax, *hate speech*, prostitusi online, jual beli narkoba online, judi online, terorisme, pornografi anak, penipuan, dan bahkan kejahatan hingga lintas batas negara

[1]Petrus Reinhard Golose, *Seputar Kejahatan Hacking*, (Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian, 2008), hlm. 25

[2] Susan W. Brenner. *Cybercrime Criminal Threats from Cyberspace*. (United State of America: Praeger, 2010), hal. 39-47

[3]https://www.kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan_media, diakses tanggak 30 Agustus 2024

[4] https://www.kemlu.go.id/id/kebijakan/isu-khusus/Pages/Penanggulangan-Kejahatan-Lintas-Negara-Teroganisir.aspx diakses pada 1 September 2024

sudah menjadi penyakit baru di masyarakat Indonesia bahkan juga internasional. *Cybercrime* telah menjadi ancaman serius terhadap keamanan dan kemakmuran global. Hal ini karena *cybercrime* merupakan kejahatan tanpa batas yang dapat melintasi batas negara yang disebut dengan kejahatan transnasional (*transnational crime)*. Kejahatan transnasional dipandang sebagai salah satu ancaman serius terhadap keamanan global yang dituntut dalam yurisdiksi hukum nasional suatu negara, kejahatan transnasional tidak berada dalam yurisdiksi peradilan internasional karena salah satu unsur dari transnasional adalah adanya lintas batas negara, sehingga untuk menghadapi kejahatan transnasional diperlukan kerjasama antar negara untuk saling bantu-membantu dalam menyelesaikan proses penegakan hukum.[5]

Kejahatan lintas negara memiliki karakteristik cukup sulit untuk diselidiki. Para ahli kriminologi belum ada secara eksplisit memberikan definisi *transnational crime*. Namun, penulis mengutip definisi *transnational crime* yang akan memberikan gambaran umum sebagai berikut:

Transnational crime is international crime, crimes that are defined by international (criminal) law. Transnational crimes have to do with crimes that are commissioned in more than one country, crossing national borders. Activities can be illegal in all nations where they occurred, or in one or more but not all countries (for instance in one country alcohol is forbidden by criminal law but not in its adjacent neighbors. Transnational crime are about transferring legal and illegal goods and providing illegal service, illegal to other countries but also includes forms of contemporary cybercrime on the internet.[6]

Dari defenisi tersebut di atas dapat disimpulkan bahwa kejahatan transnasional adalah kejahatan internasional, kejahatan yang dilakukan dengan melibatkan lebih dari satu negara atau lintas batas negara. Kegiatan dapat ilegal di semua negara di mana kejahatan terjadi, atau dalam satu atau lebih tetapi tidak semua negara termasuk bentuk kejahatan melalui internet.

Dewasa ini, Indonesia sedang dihadapkan dengan sistuasi semakin cepat dan berkembangnya teknologi informasi. Data menunjukkan bahwa tingkat kasus *cybercrime* di Indonesia meningkat drastis rentang waktu tahun 2021-2022 terjadi peningkatan kasus dari 621 kasus menjadi 8.831 kasus. Berdasarkan penanganan kasus *cybercrime* yang dilakukan oleh Kepolisian Republik

[5] Shidqi Noer Salsa. Mutual Legal assistance in the investigation of the criminal action of human trade through Social Media transnational organized Crime. Jurnal Yuridis, Vol. 8 No.1, Juni 2021: 1-22
[6] Gerben Bruinsma. *Histories of Transnational Crime*. (New York: Springer, 2015), Hlm:1

Indonesia melalui Unit Patroli Siber[7], merilis beberapa jenis *cybercrime* yang terjadi di wilayah hukum Indonesia yaitu:

a. Peretasan (*hacking*)
b. Penyadapan illegal (*illegal interception*)
c. Gangguan sistem
d. Manipulasi data
e. Pornografi *online*
f. Judi *online*
g. Pemerasan dalam jaringan (*online extortion*)
h. Ujaran kebencian
i. Pengancaman dalam jaringan (*online threat*)
j. Akses illegal
k. Pencurian data (*data theft*)

Dalam "Strain theory", Robert K. Merton mengatakan *crime is a product of society, individual commit crimes because they cannot succeed within the boundaries society has created for them*[8], yang secara sederhana dapat diartikan bahwa individu melakukan kejahatan karna ketidakmampuan mengikuti batas-batas yang dibuat oleh masyarakat itu sendiri. Sebagai contoh kasus *cybercrime* dalam lingkup *transnational crime*, pada bulan Juli 2017, beberapa sistem keamanan milik pemerintah maupun swasta diserang oleh virus Ransomware WannaCry. Di Indonesia, serangan ini terjadi di Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais. Selain itu, menurut keterangan Menteri Komunikasi dan Informatika Rudiantara Ransomware WannaCry yang terjadi di Indonesia juga menyerang ribuan alamat Internet Protocol (IP), serangan Ransomware WannaCry tak hanya menimpa komputer yang ada di ibu kota, namun juga di sejumlah daerah. Ribuan komputer yang disandera oleh Ransomware WannaCry berasal dari sektor perkebunan, manufaktur, dan perbankan yang berada di daerah. Selain itu, juga menerima laporan bahwa Samsat di Sulawesi turut menjadi korban keganasan Ransomware WannaCry.[9] 21 januari 2022 virus

[7]https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat, diakses tanggal 2 September 2024
[8]Kathleen Currul Dykeman and Susan Guarino Ghezzi. Crime. Dalam Investigating Social Problems. London: Sage tahun 2015 hal, 295.
[9] https://www.cnnindonesia.com/teknologi/20170516161343-185-215269/ribuan-alamat-ip-di-indonesia-jadi-korban-wannacry diakses pada 4 September 2024

Ransomware Conti juga menyerang beberapa komputer milik Bank Indonesia cabang Bengkulu. Selain itu juga kasus serupa juga terajdi pada tahun 2023, terjadi pemerasan dengan meretas sistem layanan Bank Syariah Indonesia (BSI) sehingga menggangu layanan bank sejak 8 Mei 2023-11 Mei 2023. Serangan ransomware yang dialami oleh BSI diklaim dilakukan oleh kelompok peretas "lockbit", kelompok peretas ini terorganisir dan sudah tersebar di beberapa negara. Dan yang menggemparkan Pada bulan Juni tahun 2024 Pusat Data Nasional Sementara Indonesia diserang oleh *ramsonware brain cipher*. Semua serangan *ransomware* tersebut diklaim dilakukan oleh oganisasi peretas internasional.

METODE PENELITIAN

Metode penelitian yang Penulis gunakan untuk memecahkan isu masalah pada tulisan ini adalah dengan menggunakan qualitative method dalam pengumpulan dan pengelolaan data penelitian. Data yang telah Penulis peroleh dianalisis dan dirangkum dalam bentuk deskriptif. Pengumpulan dokumen kualitatif berupa dokumen publik, putusan pengadilan, koran, makalah, laporan dan studi literature kepustakaan serta peraturan-peraturan internasional dan nasional.

PEMBAHASAN

Malware merupakan singkatan dari *malicious software* yaitu perangkat lunak jahat yang mencakup semua hal-hal buruk yang masuk ke komputer. *Malware* mencakup *ransomware*, virus dan worm, Trojans, backdoors, merujuk ke perangkat lunak yang dirancang untuk membahayakan atau mengganggu komputer dengan cara tertentu. Malware menyebarkan dan menginfeksi sistem komputer dengan berbagai cara. Malware yang paling umum dikenal adalah Virus. Bahkan, beberapa orang menggunakan istilah virus sebagai sebutan untuk perangkat lunak berbahaya daripada menyebutnya malware. Virus komputer mampu mereplikasi dirinya sendiri dan menyebar, virus biasanya akan membuat salinan dirinya sendiri, atau mengintegrasikan dirinya dengan file dan sistem yang terinfeksi.

Berikut adalah tiga contoh malware yang sering/umum muncul dikomputer:

1. **Mytob.** Mytob adalah kombinasi dari Mydoom e-mail worm dan Internet Relay Chat (IRC) yang terkontrol backdoor. Selain menyebar melalui e-mail, Mytob juga dapat menyebar dengan cara

scanning, dan exploiting, remote vulnerabilities. Beberapa bisa menyebar menggunakan MSN Messenger atau Windows Messenger.

2. **Netsky**. Netsky biasanya menyebar melalui e-mail atau melalui jaringan file sharing P2P. Malware memindai dan menyebar berbagai jenis file melalui e-mail.
3. **Sober**. Sober adalah rekayasa berupa dukungan teknis atau help desk personil dari domain yang sama dengan komputer pengguna membuat banyak pengguna, membuka lampiran file yang tidak diketahui. Seperti Netsky, Sober menyebar melalui e-mail ke alamat yang didapat yang telah terinfeksi.

Chang-Tsun LI (2010) membagi jenis- jenis kejahatan malware sebagai berikut:

1. Trojan horse.
2. Keyloggers.
3. Downloader
4. Spyware
5. Traffic redirectors
6. Password harvesters
7. Backdoors

Akibat bahaya *malware* tersebut sehingga banyak berbagai aplikasi anti *malware* yang ditawarkan. Namun, tak sedikit yang disalahgunakan untuk menyebar *malware* itu sendiri melalui anti *malware* palsu yang sebenarnya bukan anti *malware* melainkan *malware.* Seperti contoh, Antivirus ***System Pro*** adalah anti-*spyware* nakal yang menggunakan hasil pemindaian palsu, peringatan keamanan palsu, dan pembajakan Internet Explorer yang sebenarnya bukan antivirus. Antivirus ini akan terus-menerus memberi peringatan keamanan palsu yang menyatakan bahwa komputer pengguna diserang atau komputer telah terinfeksi virus. Kemudian akan meminta pengguna untuk memindai komputer dan mengkliknya, secara otomatis akan meluncurkan Antivirus *System Pro* dan kemudian meminta pengguna untuk membelinya. Antivirus System Pro akan menginstal Internet *Explorer Browser Helper Object* yang akan membajak *Internet Explorer* sehingga ketika pengguna *browsing situs web* akan kembali ditunjukkan pesan peringatan.[10]

[10] https://www.bleepingcomputer.com/forums/t/274142/antivirus-system-pro-removal/, diakses tanggal 10 Oktober 2024

Ransomware is a form of malware that was made by its creators to cause problems on a PC which blocks access to information. The creators will essentially block files and demand money to give access to the information. Secara sederhana dapat diartikan bahwa *Ransomware* adalah bentuk *malware* yang dibuat oleh penciptanya untuk menimbulkan masalah pada *personal computer* (PC) yang memblokir akses ke informasi atau data yang ada sistem perangkat komputer. Pencipta pada dasarnya akan memblokir file dan meminta uang sebagai tebusan untuk memberikan akses kembali ke informasi yang disabotase oleh peretas.[11]

Adapun Cara kerja *Ransomware mensabotase dokumen atau file* sebagai berikut:

1. Membuat komputer target menjadi terinfeksi
2. Kemudian dilakukan ke komputer pusat untuk mengakses informasi yang diperlukan untuk memulai program *ransomware*;
3. Semua file dienkripsi;
4. Sebuah pesan kemudian diposting meminta pembayaran untuk mendekripsi file;
5. Menerapkan metode *double extortion,* meminta sejumlah tebusan yang harus dibayar atau mengancam akan kehilangan informasi.[12]

Berkembangnya berbagai *transnational crime* yang melibatkan antar negara menjadi perhatian oleh negara-negara di dunia. Dalam hal ini *cybercrime,* serangan *malware ransomware*. Kejahatan tersebut tidak hanya dilakukan oleh individu saja namun dilakukan secara berkelompok atau terorganisir oleh kelompok kejahatan yang memiliki jaringan diberbagai negara.

Pada dasarnya *transnational crime* atau kejahatan transnasional meliputi dua aspek utama yakni:

1. Bahwa tindakan yang dilakukan oleh pelaku tersebut melanggar aturan-aturan yang ada atau hukum yang berlaku.
2. Kejahatan transnasional adalah lingkup aksi atau tindakan yang dilakukan telah melewati batas-batas negara atau lintas negara.[13]

Menyikapi kejahatan transnasional yang semakin berkembang, negara-negara yang tergabung dalam Perserikatan Bangsa-Bangsa (PBB) sepakat untuk membuat sebuah konvensi internasional yang dijadikan sebagai pedoman dalam menanggulangi *Transnational Organized Crimes* (TOC). Pada tanggal 15 Desember 2000 di Palermo, Italia lahirlah sebuah konvensi *United Nation Convention*

[11] Dale Michelson. *WannaCry Ransomware Attack: Learning the Essential*, (Copyrighted material. 2017), hlm.1
[12] Dale Michelson. *WannaCry Ransomware Attack: Learning the Essential*, (Copyrighted material. 2017), hlm.1
[13] Muzadi Hasyi. Kehajatan Terorisme Perspektif Agama, Ham dan Hukum. (Bandung: Rafika Aditama, 2004), hal:52

Against Transnational Organized Crime (UNTOC) atau Konvensi Palermo. Konvensi ini ditandatangani oleh 126 negara anggota PBB termasuk Indonesia.

Ruang lingkup *transnational crime* dalam Konvensi Palermo, menyatakan bahwa kejahatan bersifat transnasional jika:

a) di lebih dari satu wilayah negara;
b) di suatu negara, tetapi persiapan, perencanaan, pengarahan atau pengendalian atas kejahatan tersebut dilakukan di wilayah negara lain;
c) di suatu wilayah negara, tetapi melibatkan suatu kelompok pelaku tindak pidana yang terorganisasi yang melakukan tindak pidana di lebih dari satu wilayah negara; atau
d) di suatu wilayah negara, tetapi akibat yang ditimbulkan atas tindak pidana tersebut dirasakan di negara lain.

Berdasarkan artikel 2 poin a UNTOC, disebutkan bahwa definisi kelompok kriminal yang menjadi aktor dari TOC merupakan:

"Kelompok pelaku tindak pidana terorganisasi" berarti suatu kelompok terstruktur yang terdiri dari tiga orang atau lebih, terbentuk dalam satu periode waktu dan bertindak secara terpadu dengan tujuan untuk melakukan satu tindak pidana serius atau pelanggaran atau lebih yang ditetapkan menurut Konvensi ini, untuk mendapatkan, secara langsung atau tidak langsung, keuntungan keuangan atau materi lainnya.

Dari definisi di atas menunjukkan bahwa sindikat kelompok kriminal mempunyai peranan penting dalam berkembangnya TOC. Hal ini menjadi perhatian serius antar negara mengingat pelaksanaan dari kejahatan cukup sulit dilacak karena telah terorganisasi dengan baik mulai dari persiapan hingga pengawasan berjalannya rangkaian kejahatan. Sehingga tindakan tersebut termasuk dalam kejahatan serius sebagaimana disebutkan dalam Artikel 2 poin b Konvensi Palermo: "*Serious crime shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty*"

Konvensi ini merupakan instrumen internasional pertama yang mengikat secara hukum khusus tertuju pada masalah kejahatan transnasional terorganisir namun hanya bersifat mengikat negara bukan warganegaranya. Meskipun konvensi ini bersifat internasional namun konvensi ini digunakan untuk menanggulangi kejahatan nasional suatu negara bukan untuk kejahatan internasional.

Kemampuan teknologi informasi menghubungkan seluruh masyarakat dari berbagai belahan membuat siapa saja berpotensi menjadi korban dan pelaku *cybercrime.* Sehingga wajar apabila *cybercrime* dimasukkan ke dalam jenis kejahatan yang sifatnya internasional. Untuk menguatkan pernyataan tersebut, penulis mengutip pendapat Albanese yang menyebutkan dalam bukunya bahwa Perserikatan Bangsa-Bangsa (PBB) menetapkan 18 kategori kejahatan transnasional yaitu:

1. *Money laundering*
2. *Terrorist activities*
3. *Theft of art and cultural objects*
4. *Theft of intellectual property*
5. *Illicit traffic in arms*
6. *Sea piracy*
7. *Hijacking on land*
8. *Insurance fraud*
9. *Computer crime (cybercrime*)
10. *Environmental crime*
11. *Trafficking in persons*
12. *Trade human body parts*
13. *Illicit drug trafficking*
14. *Fraud bankruptcy*
15. *Infiltration of legal business*
16. *Corruption*
17. *Bribery of public officials*
18. *Other offences committed by organized criminal groups.*[14]

Selain PBB, negara-negara di ASEAN[15] juga membuat kesepakatan untuk memerangi kejahatan transnasional di negara-negara ASEAN. Negara-negara ASEAN merupakan negara-negara berkembang yang sarat akan kejahatan. Negara-negara yang tergabung dalam ASEAN mengadakan

[14] Philip Reichel & Jay Albanese, *Transnational Crime and Justice*, (California: SAGE Publications, Inc, 2014) hal. 6-7
[15] Organisasi antar-pemerintah menekankan pada kesetaraan, bersifat koordinatif dan bukan organisasi supranasional yaitu pengambilan keputusan dilakukan oleh perwakilan pemerintah, dan dalam hal-hal tertentu pemerintah dari masing-masing negara anggota tersebut tidak bisa dinyatakan terikat ketika mereka tidak menghendaki. Dyan Franciska Dumaris Sitanggang. Implementasi Personalitas Hukum Internasionalaseandalam Pembentukan Perjanjian Internasional. Jurnal Yuridis Vol. 7 No. 2, Desember 2020: 372-404

pertemuan yaitu Konferensi ASEAN pertama tentang Kejahatan Transnasional diadakan di Manila pada 18-20 Desember 1997. Pada pertemuan tersebut menghasilkan *ASEAN Declaration on Transnational Crime* Manila, Philippines, 20 *December* 1997. Salah satu agenda yang dihasilkan menyusun strategi untuk memerangi kejahatan transnasional, sebagai berikut:

1. Memperkuat komitmen Negara-negara Anggota untuk bekerja sama di tingkat regional dalam memerangi kejahatan transnasional;
2. Mengadakan setidaknya satu kali dalam dua tahun *ASEAN Ministerial Meeting* tentang Kejahatan Transnasional untuk mengoordinasikan kegiatan badan-badan ASEAN yang relevan, seperti *ASEAN Senior Officials on Drug Matters (ASOD* dan *ASEAN Chiefs of National Police (ASEANAPOL*);
3. Mengadakan diskusi dengan maksud untuk menandatangani perjanjian bantuan hukum timbal balik, perjanjian bilateral, nota kesepahaman atau pengaturan lain di antara Negara-negara Anggota;
4. Mempertimbangkan pembentukan *ASEAN Centre on Transnational Crime (ACOT)* yang akan mengoordinasikan upaya regional melawan kejahatan transnasional melalui pembagian intelijen, harmonisasi kebijakan dan koordinasi operasi;
5. *Convene a high-level ad-hoc Experts Group* dalam satu tahun untuk menyelesaikan hal-hal berikut dengan bantuan dari Sekretariat ASEAN:
    a. *ASEAN Plan of Action on Transnational Crime,*
    b. *Institutional Framework for ASEAN Cooperation on Transnational Crime, and,*
    c. *Feasibility study on the establishment of ACOT*;
6. Mendorong Negara-negara Anggota untuk mempertimbangkan penempatan Polisi dan/atau Petugas Penghubung Polisi di ibukota masing-masing untuk memfasilitasi kerja sama untuk menangani kejahatan transnasional;
7. Mendorong jejaring lembaga atau organisasi nasional yang relevan di Negara-Negara Anggota yang berurusan dengan kejahatan transnasional untuk lebih meningkatkan pertukaran informasi dan diseminasi;
8. Perluas ruang lingkup upaya Negara-negara Anggota terhadap kejahatan transnasional seperti terorisme, peredaran gelap narkoba, penyelundupan senjata, pencucian uang, lalu lintas

orang dan pembajakan, dan untuk meminta Sekretaris Jenderal ASEAN untuk memasukkan bidang-bidang ini dalam program kerja Sekretariat ASEAN;

9. Jelajahi cara-cara di mana Negara-negara Anggota dapat bekerja lebih dekat dengan lembaga dan organisasi terkait di negara-negara *Dialogue Partner*, negara-negara lain dan organisasi internasional, termasuk PBB dan lembaga-lembaga khususnya, *Colombo Plan Bureau*, Interpol dan lembaga-lembaga lainnya untuk memerangi kejahatan transnasional
10. Bekerjasama dan berkoordinasi lebih erat dengan badan-badan ASEAN lainnya seperti para *ASEAN Law Ministers and Attorneys-General*, Kepala Polisi Nasional ASEAN, Para Menteri Keuangan ASEAN, Direktur Jenderal Imigrasi dan Direktur Jenderal Bea Cukai dalam penyelidikan, penuntutan dan rehabilitasi para pelaku kejahatan transnasional; dan,
11. Memperkuat kapasitas Sekretariat ASEAN untuk membantu Negara-negara Anggota dalam memulai, merencanakan, dan mengkoordinasikan kegiatan, strategi, program dan proyek untuk memerangi kejahatan transnasional[16].

Masalah *cybercrime* pada dasarnya bukan masalah baru yang timbul pada tahun 2000-an, namun *cybercrime* sudah ada sejak tahun 1990-an. *Cybercrime* terjadi pertama kali di Amerika Serikat, pada tahun 1971 sampai 1985 Stanford Research International (SRI) melakukan penelitian terkait bentuk-bentuk *cybercrime* di Amerika Serikat. Dalam penelitian tersebut ditemukan 1600 kasus yang terjadi sejak tahun 1958, namun kasus tersebut diselesaikan secara perdata. Dalam penelitian yang dilakukan belum menunjukkan pengaturan *cybercrime* dalam hukum pidana sehingga *cybercrime* belum dimasukkan dalam statistik kriminal. Sementara *cybercrime* di Indonesia telah ada sejak tahun 1983 yaitu kasus pembobolan Bank Rakyat Indonesia (BRI) Cabang Brigjen Katamso Yogyakarta. Kemudian pada tahun 1986 terjadi pembobolan Bank Negara Indonesia 1946 (BNI 1946) dengan cara menggunakan fasilitas komputer.[17]

Di era industrialisasi, perkembangan teknologi informasi membuat hubungan antar negara bersifat mendunia yang menciptakan tata dunia baru. Dan juga menimbulkan beragam kejahatan yang semakin kompleks. Masalah pembuktian dalam *cybercrime* menjadi masalah yang cukup krusial dan sulit sampai saat ini. Mengingat karakteristik dari *cybercrime* yang identik dengan komputer sehingga dalam pengumpulan bukti membutuhkan alat teknologi yang canggih. Interaksi

[16] *ASEAN Declaration on Transnational Crime* Manila, 20 December 1997, ASEAN Ministerial Meeting on Transnational Crime (AMMTC) I
[17]Widodo. *Aspek Hukum Pidana Kejahatan Mayantara*, (Yogyakarta ;AswajaPressindo,2013) hal. 40-41

yang berbeda-beda antara konteks kejahatan, jenis, kuantitas, dan kualitas bukti membentuk lanskap investigasi kriminal. Mengenali perbedaan yang melekat dalam nilai bukti merupakan hal mendasar untuk membangun kasus yang meyakinkan. Seiring kemajuan teknologi dan berkembangnya metodologi forensik, upaya mencapai keadilan menuntut pendekatan holistik dan adaptif untuk menguraikan hubungan antara orang, tempat, dan benda setelah terjadinya kejahatan.[18]

Namun, *cybercrime* dalam konteks kejahatan transnasional masalah yang paling krusial bukan terletak pada masalah pembuktian tetapi terletak pada yurisdiksi. Sebagaimana Penulis mengutip bahwa:

Yurisdiksi merupakan wewenang negara melalui badan peradilan negara yang bersangkutan untuk mengadili dalam batas wilayah hukum pengadilan tersebut atau wewenang negara atas semua orang atau benda yang berada di dalam batas teritorial negara. Yurisdiksi merupakan salah satu aspek kedaulatan negara meliputi kewenangan judisial, legislatif dan administrative.[19]

Dalam praktik hukum internasional Criyer cs membagi 3 (tiga) model atau lingkup yurisdiksi yaitu:

a. Yurisdiksi legislatif (*legislative jurisdiction*) adalah wewenang badan legislatif untuk menetapkan suatu undang-undang yang berlaku baik di dalam maupun di luar batas teritorial dari negara yang bersangkutan.
b. Yurisdiksi pengadilan (*adjudicative jurisdiction*) adalah wewenang pengadilan terhadap kasus-kasus kejahatan transnasional atau kejahatan internasional.
c. Yurisdiksi eksekutif adalah kebijakan eksekutif (Presiden) untuk memerintahkan penangkapan dan penahanan seseorang pelaku kejahatan yang merupakan ancaman terhadap keamanan dan kedaulatan suatu negara.[20]

Yurisdiksi menyangkut terhadap kedaulatan negara dan kedaulatan hukum. Konsep kedaulatan merupakan hak absolut yang dimiliki suatu negara. Sebagaimana menurut

[18] Handar Subhandi Bakhtiar. The Role And Nature Of Evidence: Forensic Insight. Jurnal Yuridis. Volume: 10 Nomor: 2, Desember 2023, Hal:18
[19]Romli Atmasasmita. *Ekstradisi dalam Meningkatkan Kerja Sama Penegakan Hukum*. Jurnal Volume 5 Nomor 1 Oktober 2007 hal.108
[20]*Ibid*, hal.108-109

pendapat Jean Bodin bahwa kedaulatan sebagai kekuasaan yang absolut dan berkelanjutan dalam sebuah negara yang berada di atas hukum positif.[21]

Untuk menyelesaikan kasus *cybercrime* dalam konteks transnasional diperlukan suatu kerjasama bilateral maupun multilateral suatu negara untuk sama-sama menerapkan prinsip *double criminality*[22] terhadap *cybercrime.* Berlakunya hukum pidana suatu negara tidak dapat diterapkan begitu saja di negara lain. Setiap negara harus menghormati yurisdiksi negara lain. Hemat Penulis Yurisdiksi kiriminal yaitu asas berlakunya hukum pidana suatu negara menurut ruang tempat dan orang terbagi menjadi 4 (empat) asas [23] yaitu:

a. Asas Teritorialitas atau Wilayah

Menurut asas ini hukum pidana suatu negara berlaku di wilayah negara itu sendiri. Asas ini menunjukkan bahwa siapa pun yang melakukan delik di wilayah negara tempat berlakunya hukum pidana tunduk pada hukum pidana tersebut.

b. Asas Perlindungan atau Asas Nasionalitas Pasif

Asas ini menentukan bahwa hukum pidana suatu negara berlaku terhadap perbuatan-perbuatan yang dilakukan di luar negeri, jika karena itu kepentingan tertentu terutama kepentingan negara dilanggar di luar wilayah kekuasaan negara itu. Dalam asas ini yang dilindungi bukanlah kepentingan individual melainkan kepentingan nasional atau kepentingan umum yang lebih luas.

c. Asas Personalitas atau Asas Nasionalitas aktif

Asas ini bertumpu pada kewarganegaraan pembuat delik. Hukum pidana Indonesia mengikuti warganegaranya dimana pun berada.

d. Asas universalitas

[21]Munir Fuady, *Teori-Teori Besar (Grand Theory) Dalam Hukum.* Jakarta: Kencana Prenadamedia Gropup, 2014, hal. 91-92

[22] *The principle of double criminality or dual criminality has long been applied, requiring that the underlying act or omission is criminal in both the requesting and the requested state. The principle stems from the principle of legality (nulla poena sine lega), but it also closely linked to stet sovereignty and reciprocity. It is often asserted that the requirement, although sometimes discretionary, constitutes a major obstacle to effective cooperation and many commentators argue that is no longer necessary, other ground for refusal, such as ordre public[22], offer sufficient protection of state interest.* Robert Cryer, et al. *An Introduction to International Criminal Law and Procedure Second Edition*, (New York: Cambridge University Press, 2010), hal. 89

[23]A. Z. Abidin & Andi Hamzah. *Pengantar Dalam Hukum Pidana Indonesia*. Jakarta: PT Yarsif Wtampone, 2010, hal. 83-93

Asas ini melihat hukum pidana berlaku umum melampaui batas ruang wilayah dan ruang orang. Pada asas ini yang dilindungi adalah kepentingan dunia atau global. Asas ini berlaku terhadap kejahatan luar biasa yang mengancam kepentingan dunia secara universal atau menyeluruh.

Menurut Cassese membagi asas universal yaitu asas universal yang absolut dan asas universal yang sempit/terbatas. Asas universal yang absolut adalah setiap negara dapat melaksanakan kewenangannya menuntut seseorang yang dituduh melakukan kejahatan internasional tanpa harus mempertimbangkan kewarganegaraan yang bersangkutan, *locus delicti* kejahatan dan kewarganegaraan korban, bahkan tanpa harus mempertimbangkan apakah tertuduh berada di bawah kekuasaan negara tertentu atau tidak. Sedangkan asas universal yang terbatas adalah hanya negara dimana tertuduh berada di wilayah yurisdiksi negara yang bersangkutan yang dapat menuntut tersangka yang bersangkutan (atau forum *deprehensionis*). Berdasarkan asas universal yang terbatas ini keberadaan tertuduh di dalam wilayah negara yang bersangkutan merupakan syarat kewenangan untuk menuntut dan mengadili.[24]

Asas-asas tersebut di atas juga berlaku dalam hukum pidana internasional. Pada prinsipnya asas yang berlaku hukum pidana nasional juga berlaku dalam pidana internasional. Dalam konteks kejahatan transnasional berbeda dengan kejahatan internasional, meskipun kejahatan transnasional bersifat internasional. Perbedaan itu terletak pada hukum yang mengatur dan delik yang diatur. Dalam hukum internasional telah disepakati yurisdiksi penyelesaian apabila terjadi kejahatan genosida, kejahatan kemanusiaan, kejahatan perang dan kejahatan agresi[25] yaitu melalui Mahkamah Pidana Internasional (*International Criminal Court*/ICC). Sedangkan kejahatan transnasional belum tentu yurisdiksi yang pasti dalam penyelesaiannya, karena setiap negara memiliki hukum atau aturan yang berbeda. Dalam penyelesaian kejahatan diperlukan hubungan kerja sama.

Contoh kasus *cybecrime* yang bersifat *transnational crime* dapat dibedah melalui serangan Malware *Ransomware Wannacry* yang terjadi di Indonesia pada bulan Mei tahun 2017 Rumah sakit Harapan Kita dan Rumah Sakit Dharmais. Pada kasus ini yang terdampak bukan hanya negara Indonesia namun ada 150 negara. Jika dikaitkan dengan Asas Teritorialitas atau Wilayah, maka

[24]Romli Atmasasmita, *Hukum Pidana Internasional Dalam Kerangka Perdamaian dan Keamanan Internasional*, Jakarta: PT Fikahati Aneska, 2010, hal. 133-134
[25]*Ibid*, hal. 156

semua negara yang terdampak mempunyai kewenangan untuk mengadili pelaku. Hal ini logis, karena setiap negara berhak melindungi kepentingan negaranya dari setiap delik yang terjadi di wilayahnya. Tetapi menjadi tidak logis jika semua negara mengadili pelaku yang tentu memiliki hukum dan hukuman yang berbeda. Sedangkan jika dianalisis berdasarkan Asas Nasionalitas Pasif atau Asas Perlindungan dan Asas Personalitas atau Asas Nasionalitas tidak jauh berbeda dengan Asas Teritorialitas atau Wilayah, hanya saja kemungkinan kejahatan/delik yang diatur yang berbeda. Seperti contoh dalam tata hukum Indonesia pemberlakuan hukum pidana nasional berdasarkan Asas Nasionalitas Pasif atau Asas Perlindungan dan Asas Personalitas atau Asas Nasionalitas aktif hanya berlaku terhadap kejahatan-kejahatan tertentu yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP), tidak serta merta semua kejahatan dapat memberlakukan asas ini. Sementara di negara lain belum tentu kejahatan yang diatur di Indonesia tersebut sama atau kemungkinan tidak diatur sama sekali. Sedangkan jika di analisis berdasarkan Asas Universalitas, dimana hukum pidana berlaku umum melampaui batas ruang wilayah dan ruang orang. Pada asas ini yang dilindungi adalah kepentingan dunia atau global. Asas ini berlaku terhadap kejahatan luar biasa yang mengancam kepentingan dunia secara universal atau menyeluruh. Hemat penulis, asas ini lebih tepat digunakan terhadap kejahatan internasional

PENUTUP

Penyelesaian kasus serangan Malware Ransomware sebagai bentuk *cybercrime* dalam perspektif *transnational crime*, dapat menggunakan Konvensi Palermo atau UNTOC. Namun, UNTOC tidak mempunyai kekuatan hukum apabila tidak diratifikasi suatu negara, artinya Konvensi ini hanya terikat terhadap negara yang meratifikasinya. Tidak serta merta UNTOC berlaku universal terhadap semua negara di dunia. Bisa dikatakan UNTOC adalah perjanjian atau kerjasama internasional negara-negara di dunia. Menurut Koesnadi Kartasasmita, kerjasama internasional terjadi karena adanya *national understanding* serta mempunyai tujuan yang sama, keinginan yang didukung oleh kondisi internasional yang saling membutuhkan.[26] Sebagaimana tercantum dalam Konvensi Palermo menyatakan bahwa “Konvensi ini berlaku dengan adanya ratifikasi, penerimaan atau persetujuan”. Negara-negara yang meratifikasi UNTOC wajib menetapkan dalam undang-

[26]Koesnadi Kartasasmita, *Administrasi Internasional* (Bandung: Lembaga Penerbitan Sekolah Tinggi Ilmu Administrasi, 1997), hal. 20

undang nasionalnya apa yang diatur dalam UNTOC. Dalam artian UNTOC berlaku sebagai panduan bagi negara peratifikasi dalam menyusun atau membuat undang-undang nasionalnya terkait. Oleh karena itu penegakan hukum terhadap kejahatan transnasional yang berlaku adalah hukum nasional suatu negara bukan hukum internasional.

DAFTAR PUSTAKA

Abidin, A. Z. & Andi Hamzah. *Pengantar Dalam Hukum Pidana Indonesia*. Jakarta: PT Yarsif Wtampone. 2010

Atmasasmita, Romli. Hukum Pidana Internasional Dalam Kerangka Perdamaian dan Keamanan Internasional. Jakarta: PT Fikahati Aneska. 2010

Atmasasmita, Romli. *Ekstradisi dalam Meningkatkan Kerja Sama Penegakan Hukum*. Jurnal Volume 5 Nomor 1 Oktober 2007

Bakhtiar, Handar Subhandi. *The Role and Nature of Evidence: Forensic Insight*. Jurnal Yuridis. Volume: 10, Nomor: 2, Desember 2023

Brenner, Susan W. *Cybercrime Criminal Threats from Cyberspace*. United State of America: Praeger. 2010

Bruinsma, Gerben. *Histories of Transnational Crime*. New York: Springer. 2015

Dykeman, Kathleen Currul and Susan Guarino Ghezzi. 2015. Crime. Dalam Investigating Social Problems. London: Sage

Dyan Franciska Dumaris Sitanggang. Implementasi Personalitas Hukum Internasionalaseandalam Pembentukan Perjanjian Internasional. Jurnal Yuridis Vol. 7 No. 2, Desember 2020: 372-404

Fuady, Munir. *Teori-Teori Besar (Grand Theory) Dalam Hukum*. Jakarta: Kencana Prenadamedia Gropup. 2014

Golose, Petrus Reinhard. *Seputar Kejahatan Hacking*, (Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian. 2008

Hasyi, Muzadi Hasyi. 2004. Kehajatan Terorisme Perspektif Agama, Ham dan Hukum. Bandung: Rafika Aditama

https://www.kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan_media, diakses tanggal 30 Agustus 2024

https://www.kemlu.go.id/id/kebijakan/isu-khusus/Pages/Penanggulangan-Kejahatan-Lintas-Negara-Teroganisir.aspx, diakses tanggal 1 September 2024

https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat, diakses tanggal 2 September 2024

https://www.cnnindonesia.com/teknologi/20170516161343-185-215269/ribuan-alamat-ip-di-indonesia-jadi-korban-wannacry, diakses tanggal 4 September 2024

https://www.bleepingcomputer.com/forums/t/274142/antivirus-system-pro-removal/, diakses tanggal 10 Oktober 2024

Kartasasmita, Koesnadi. *Administrasi Internasional* (Bandung: Lembaga Penerbitan Sekolah Tinggi Ilmu Administrasi. 1997

Michelson, Dale. *WannaCry Ransomware Attack: Learning the Essential*, (Copyrighted material). 2017

Reichel ,Philip & Jay Albanese. *Transnational Crime and Justice*. California: SAGE Publications, Inc. 2014

Robert Cryer, et al. *An Introduction to International Criminal Law and Procedure Second Edition*. New York: Cambridge University Press. 2010

Shidqi Noer Salsa. *Mutual Legal assistance in the investigation of the criminal action of human trade through Social Media transnational organized Crime*. Jurnal Yuridis, Vol. 8 No.1, Juni 2021: 1-22

Widodo. *Aspek Hukum Pidana Kejahatan Mayantara*. Yogyakarta: AswajaPressindo. 2013