Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.5. No.1 (2024)
Tema/Edisi : Hukum Internasional (Bulan Kesatu)
https://jhlg.rewangrencang.com/

ANALISIS PERAN ICC DALAM PENUNTUTAN KEJAHATAN SIBER CRIME INTERNASIONAL DALAM PRAKTIK HUKUM PIDANA INTERNASIONAL

ANALYSIS OF THE ROLE OF THE ICC IN THE PROSECUTION OF INTERNATIONAL CYBERCRIMES IN THE PRACTICE OF INTERNATIONAL CRIMINAL LAW

Zaenudin, Mohamad Ali, Andre Subandrio dan Siti Marina
Legal Studies Program, University Bina Bangsa
Email: Zayzayganteng@.gmail.com,
Citation Structure Recommendation: Zaenudin, Mohamad Ali, Andre Subandrio dan Siti Marina. *Analisis Peran ICC dalam Penuntutan Kejahatan Siber Crime Internasional dalam Praktik Hukum Pidana Internasional*. Jurnal Hukum Lex Generalis. Vol.5. No.1 (2024).

ABSTRAK

Kejahatan dunia maya telah menjadi ancaman signifikan di era digital, memengaruhi keamanan global, stabilitas ekonomi, dan hak asasi manusia. Sifat lintas batas kejahatan dunia maya seringkali melebihi kemampuan yurisdiksi nasional untuk menanganinya, menciptakan kebutuhan akan mekanisme internasional yang efektif. Ditemukan bahwa, meskipun Statuta Roma belum mencakup kejahatan dunia maya, ada peluang untuk memasukkan kejahatan ini sebagai bagian dari perkembangan masa depan dalam hukum pidana internasional. Penelitian ini akan menganalisis Manfaat di International Criminal Court (ICC) dalam menuntut kejahatan dunia maya internasional dalam konteks dan hukum pidana internasional. Karena kejahatan dunia maya semakin kompleks dan terjadi lintas batas, dan telah menjadi tantangan global yang signifikan. Namun, hingga saat ini, Statuta Roma yang menjadi dasar hukum ICC belum secara eksplisit mencakup kejahatan siber seperti kejahatan besar lainnya terhadap negara-negara internasional, misalnya kejahatan terhadap genosida, kejahatan terhadap kemanusiaan dan kejahatan dalam melawan perang atau kejahatan agresi. Penelitian ini mengeksplorasi peran potensial ICC dalam menangani kejahatan dunia maya melalui interpretasi hukum pidana internasional saat ini.

Kata Kunci: ICC, Kejahatan Cyber, Hukum Pidana Internasional, Statuta Roma, Yurisdiksi

ABSTRACT

Cybercrime has become a significant threat in the digital era, affecting global security, economic stability and human rights. The cross-border nature of cybercrime often exceeds the ability of national jurisdictions to deal with it, creating the need for effective international mechanisms. It found that, although the Rome Statute does not yet cover cybercrime, there is an opportunity to include this crime as part of future developments in international criminal law. This research will analyze Benefits at the International Criminal Court (ICC) in prosecuting international cyber crimes in the context and international criminal law. Because cybercrime is increasingly complex and occurs across borders, and has become a significant global challenge. However, to date, the Rome Statute which is the legal basis for the ICC has not explicitly covered cyber crimes as other major crimes against international states, examples crimes against genocide, crimes against humanity and crimes In against war or crimes of aggression. This research explores in potential role of the ICC in dealing with cyber crimes through interpretation of current international criminal law.

Kata Kunci: ICC, Cybercrime, International Criminal Law, Rome Statute, Jurisdiction

A. PENDAHULUAN

Dalam beberapa dekade terakhir, teknologi informasi telah berkembang pesat, tetapi juga menciptakan ancaman baru dalam bentuk kejahatan siber. Kasus-kasus seperti pada serangan WannaCry, SolarWinds, serta ransomware global lainnya menunjukkan dampak destruktif pada kejahatan siber terhadap infrastruktur kritis, ekonomi, dan keamanan negara. Namun, yurisdiksi nasional sering kali terbatas dalam menangani pelaku internasional yang beroperasi di luar batas negara. International In Criminal The Court atau atau Mahkamah Terhadap Pidana Internasional yang telah diresmikan berasaskan pada Statuta Roma 1998, didirikan untuk menuntut kejahatan yang serius seperti pemakaian pada genosida, kejahatan terhadap perang, serta kejahatan terhadap kemanusiaan. [1]

Kemajuan terhadap teknologi informasi dan komunikasi dalam beberapa sepuluh tahun terakhir ini telah dapat memberikan dampak yang signifikan dalam berbagai pihak pada kehidupan, baik itu secara positif maupun secara negatif. Di sisi negatif, kemunculan kejahatan siber (cybercrime) menjadi ancaman serius bagi keamanan global. Kejahatan siber mencakup berbagai aktivitas kriminal, seperti peretasan data, penyebaran malware, serangan ransomware, hingga sabotase infrastruktur kritis negara. Kejahatan ini tidak hanya menimbulkan kerugian finansial yang masif, tetapi juga dapat mengancam stabilitas internasional, keamanan nasional, dan hak asasi manusia secara luas. Karena sifatnya yang lintas batas, kejahatan siber sering kali sulit untuk ditangani melalui mekanisme hukum domestik, sehingga membutuhkan kerjasama internasional dan pendekatan multilateral untuk penegakan hukumnya.

Di sisi lain, International In Criminal The Court (ICC), sebagai pengadilan internasional konstant yang diresmikan atas berdasarkan Statuta Roma 1998, memiliki mandat untuk dapat mengadili dan membawa kepersidangan terhadap kejahatan pada internasional paling sangat serius yang menjadi sangat perhatian pada kelompok negara-negara dunia dan negara internasional, yaitu terhadap pemabantaian atau pembunuhan menggunakan genosida itu, kejahatan terhadap kemanusiaan, kejahatan terhadap perang, serta kejahatan terhadap agresi. Namun, kejahatan siber hingga saat ini belum secara eksplisit diakui dalam yurisdiksi ICC.

[1] Pasal 5 Statuta Roma 1998.

Hal ini menimbulkan pertanyaan penting tentang bagaimana ICC dapat berperan dalam menanggulangi kejahatan siber internasional yang memiliki dampak signifikan terhadap keamanan global.[2]

Pendekatan hukum pidana internasional dalam menangani kejahatan siber masih berada pada tahap awal perkembangan. Meskipun beberapa konvensi internasional, seperti Budapest Convention on Cybercrime 2001, telah mengatur kerangka kerja untuk penanganan kejahatan siber, konvensi ini lebih berfokus pada aspek kerjasama penegakan hukum di tingkat nasional dan regional, serta belum mencakup mekanisme penuntutan dalam ranah hukum pidana internasional secara menyeluruh. Dalam konteks ini, muncul wacana untuk mengintegrasikan kejahatan siber sebagai bagian dari yurisdiksi ICC, baik melalui interpretasi hukum yang ada maupun melalui amandemen Statuta Roma.

Di sisi lain, terdapat beberapa kerangka hukum internasional yang mencoba mengatasi kejahatan siber, pada Budapest Convention on Cybercrime 2001.

Konvensi ini menjadi instrumen utama dalam mengatur kerjasama internasional untuk menanggulangi kejahatan siber, tetapi fokusnya lebih pada harmonisasi hukum domestik dan kerjasama penegakan hukum antarnegara, bukan pada mekanisme penuntutan di tingkat internasional. Hal ini menunjukkan adanya celah dalam kerangka hukum internasional yang perlu diisi untuk menghadapi tantangan kejahatan siber secara lebih efektif. Namun, upaya ini menghadapi berbagai tantangan. Pertama, terdapat persoalan yurisdiksi dan kedaulatan negara yang kompleks. Kejahatan siber sering kali melibatkan pelaku dan korban dari negara yang berbeda, sehingga sulit untuk menentukan yurisdiksi yang berwenang. Kedua, terdapat hambatan teknis dalam pengumpulan dan validasi bukti digital yang diperlukan untuk proses peradilan internasional. Ketiga, adanya resistensi politik dari beberapa negara terhadap perluasan yurisdiksi ICC, terutama yang menyangkut isu kedaulatan digital.[3]

Sehingga, tulisan ini bertujuan menganalisis peran ICC dalam penuntutan pada kejahatan siber internasional dalam praktik hukum pidana internasional.

---

[2] R Schmit dan Michael NS., *Cyber In Operations the Jus in The Bello: Key In Issues*, The International In Law Studies, Vol.90 (2014). lihat juga Statuta In Roma 1998.

[3] Jonathant B. Clought, *Principles of The Cybercrime*, The Cambridge University Press, Cambridge, 2010, p.46.

Penelitian ini sangat diharapkan dapat mengeksplorasi peluang serta tantangan yang dihadapi ICC dalam mengintegrasikan kejahatan siber ke dalam yurisdiksinya. Dengan menggunakan pendekatan normatif dan analisis kasus, penulisan ini diharapkan dapat memberikan rekomendasi bagi pengembangan serta kemajuan kerangka hukum pidana internasional yang lebih inklusif dan responsif terhadap tantangan era digital saat ini.

Untuk penelitian ini dasar rumusan masalahnya adalah sebagai berikut:

1. Apakah pada kejahatan siber crime itu dapat dikatagorikan sebagai suatu kejahatan hukum pidana internasional?
2. Apakah tantangan dan peluang bagi ICC dalam penanganan kejahatan siber crime?

Dengan uraian tersebut diatas serta dari rumsuan masalah yang penulis jabarkan, maka penulis tertarik untuk mengangkat judul dalam penulisan ini yaitu ***"Analisis Peran ICC dalam Penuntutan Kejahatan Siber Crime Internasional dalam Praktik Hukum Pidana Internasional"***

Dalam penulisan ini termasuk dalam penulisan pada hukum normatif, yang pada khususnya terfokus pada data yang diperoleh dari kepustakaan yang dijadikan sebagai kajian bahan utama. Pengertian dari hukum normatif yaitu kaidah-kaidah yang diambil dari peraturan hukum yang ada, jurnal-jurnal hasil penelitian sebelumnya dan juga kepustakaan lainnya yang berkaitan dengan penelitian ini.

B. PEMBAHASAN

1. Kategorisasi Kejahatan *Siber Crime* sebagai Suatu Kejahatan Hukum Pidana Internasional

Kemajuan pada teknologi komputer serta perangkatnya telah diikuti dengan perkembangan dari internet yang selalu membawa sejumlah dampak, yang utama dari perkembangan internet tersebut adalah terbentuknya suatu kelompok sosial atau komunitas baru dan semakin begitu pesat serta bertambah. Dari banyaknya perkembangan komunitas sosial tersebut pada media internet maka terjadinya cyberspace yang melibatkan para individu-individu (Netizen) semakin meningkat, baik itu netizen bersifat positif maupun bersifat negatif.

Dengan fakta peningkatan ini maka baik dari negara Indonesia maupun negara Internasional lainnya menganggap perlu segera diadakan suatu pengaturan tentang cyberspace beserta kegiatan-kegiatan yang dilakukannya di media internet dan dasar hukumnya. Sehingga dengan pengaturan tersebut segala kegiatan aktivitas dari siber dapat terkontrol dan teratur, dan tidak terjadinya radikalisme.

Pengertian dari kejahatan siber crime tersebut adalah suatu dari kegiatan yang dibuat dengan penggunaan teknologi informasi dan komunikasi, yang khususnya internet. Ada beberapa jenis pada kejahatan siber, yaitu:

1. Phishing atau Penipuan, yakni segala sesuatu dari jenis kejahatan pada dunia maya yang paling sering dan umum. Pada phishing ini selalu menyangkutkan keterlibatan dari email atau pesan yang palsu yang dipersiapkan untuk memperdayai objek/korban agar dapat memberikan data dan informasi baik pribadi atau perusahaan. Pada kejahatan internet, penggunaan persekongkolan sosial agar korban dapat memberikan segala informasi rahasia, seperti nomor kartu kredit, nomor rekening, kredensial login, data pribadi, keuangan & data lainnya. Biasanya pada jenis ini selalu melibatkan perangkat lunak, yaitu worm, trojan dan virus. Penipuan ini juga sering kali menggunakan identitas dari jenis perusahaan untuk dapat melakukan penipuan dan merusak keyakinan dan kepercayaan customer atau pelanggan terhadap merk tertentu dan merusak reputasi merk tersebut.
2. Penggelapan atau pencurian identitas, yaitu suatu pencurian data identitas pribadi, contohnya data transaksi yang tidak sesuai atau tidak sah yang dapat memungkinkan akan terjadinya sutu penipuan lainnya. Kejahatan pada dunia maya dengan penggunaan data informasi pribadi yang akan di curi yang digunakan dalam melakukan transaksi yang tidak sah dan aktifitas penipuan dan atau pencurian lainnya. Akibat terjadinya pencurian terhadap data identitas pribadi, maka akan terjadi beberapa dampak, yaitu :
   a) Adanya tagihan kredit elusif
   b) Terjadinya penarikan rekening bank yang tidak jelas.
   c) Terjadinya kerugian finansial
   d) Distraint Psikologis
   e) Permasalahan hukum

3. Ofensif Ransomware, yaitu serangan terhadap jaringan komputer untuk mengungkapkan arsip dari korban dan aksesnya di blokir hingga adanya tebusan yang harus dibayarkan. Pada jenis kejahatan ini merupakan pelanggaran terhadap data, dimana biasanya korban harus membayar terhadap tebusannya untuk dapat mengembalikan lagi akses sediakala. Dari hasil suatu laporan penelitian bahwa 43% organisasi dunia yang telah terkena ransomware juga pernah mengalami hal yang sama dan data tertahan atau adanya tebusan terhadap data yang telah diretas tersebut.
4. Serbuan DDOS, yaitu kepanjangan dari Distributed Denial Of Service yang artinya gempuran dari siber yang sangat masif dan berat yang sangat banyak dengan satu target khusus yaitu penghentian layanan bagi pengguna jaringan internet. Kejadian ini menempatkan pada perangkat jaringan komputer yang dibajaknya, yang biasa kita kenal dengan nama botnet untuk merilis serangan lalu lintas yang sangat besar guna membekukan atau memtaikan berbagai situs website serta layanan daring lainnya.
5. Child Pornography, yaitu penyebaran atau konsumsi ilegal terkait pada anak-anak dibawah umur, dengan memanfaatkan anak-anak tersebut dan melakukan penjualan pornograpy terhadap anak-anak.

Kejahatan pada siber crime sering melibatkan banyak negara, baik negara maju maupun negara berkembang. Pada setiap kejadian kejahatan siber crime ini selalu memakai jaringan atau sistem yang besar dan terstruktur dan sistematis dengan menggunakan jaringan komputer yang canggih, dan jaringan komputer tersebut telah dibajak, yang biasa dikenal dengan nama botnet, untuk senjata menyerang pada aplikasi komputer disetiap negara yang akan dilakukan pembajakan yang sangat besar. Walaupun belum adanya suatu perjanjian internasional yang secara jelas dalam hal pengaturan kejahatan siber, sejumlah sistem hukum telah dapat diterapkan. Salah satunya pada Konvensi Internasional untuk memberantas Kejahatan Transnasional terorganisir, Konvensi untuk memberantas pada kejahatan dari informasi, serta Kovensi Internasional untuk pencegahan dan mengatasi pada kejahatan siber merupakan suatu model pada kerangka hukum dalam penangulangan kejahatan siber secara komrehensif.

Sebagaian besar pada negara-negara dalam menghadapi kejahatan siber ini tercermin dalam perancangan undang-undang yang secara khusus untuk menaggulangi fakta serangan kejahatan siber ini. Sebagai contoh penanggulangan serangan siber pada Negara Indonesia yaitu dengan diterbitkan Undang-Undang Informasi dan Transaksi Elektronik atau yang biasa yang kita kenal dengan UU ITE. Undang-Undang ini merupakan dasar hukum bagi negara Indonesia dalam penanganan pada tindak kejahatan siber pada tingkat nasional. Pada Undang-Undang ini juga meliputi beragam macam kepastian utnuk pengaturan keamanan pada informasi, privasi data, juga berisi sanksi bagi setiap pelanggaran atas keamanan pada dunia maya. Dari pada itu, beberapa negara lainnya juga telah mengambil peraturan perundangan yang sama dengan negara Indonesia guna melindungi masyarakatnya terhadap ancaman kejahatan siber yang secara langsung. Salah contoh bisa kita lihat pada negara Inggris yang mempunyai aturan yang diberi nama Data Protection Act yang merupakan dasar rancangan hukum yang sangat berpengaruh kuat dalam perlindungan pada data pribadi dan kemanan informasi. Pearturan ini merupakan dasar yang sangat kuat dalam penegakkan hukum serta penjaminan bagi para pelaku kejahatan siber dinegara Inggris tersebut dapat berhadapan dengan aturan hukum yang sangat serius.

Selain negara Inggris, ada juga negara Amerika Serikat juga memiliki aturan huku tentang siber yang diberi nama Computer Fraud and Abuse Act (CFAA) yang merupakan yang utama sebagai perangkat hukum dalam penangulangan kejahatan siber, yang paling uatama adalah pemantauan terhadap pemakaian ilegal perangkat komputer serta pada jaringannya. Biarpun telah banyak aturan hukum di beberapa negara dalam upaya penaggulangan terhadap kejahatan siber, tetapi tetapi terlihat pada daya guna dari penegakkan aturan hukum tersebut serta penanggulanganya terhadap kejahatan siber. Penegakkan hukum harus tegas dan akan semakin sulit karena begitu cepat terjadinya perkembangan dari teknologi serta kerumitan dari serangan siber tersebut. Oleh sebab itu dalam memperbaiki dan penegakkan hukum pada setiap negara perlu selalu ada update peraturan perundangan yang berhubungan dengan siber ini, karena begitu cepatnya perkembangan terhadaop kejahatan siber ini.

Selain itu perlu diperkuat kerjasama internasional yang merupakan bagian utama dalam penangulangan pada kejahatan siber yang melewati dari batas pada suatu negara. Dengan adanya kerjasama internasional tersebut dapat saling memberikan informasi dalam pengembangan teknologi pengamanan, serta berkoordinasi terhadap aktivitas tindakan serangan pada siber.

2. Tantangan dan Peluang bagi ICC dalam Penanganan Kejahatan *Siber Crime*

Fakta dari digital informasi pada perangkat computer memiliki kekhususan yang bertentangan dari bentuk bukti fisik lazimnya. Sifatnya yang sering kali berganti, sangat mudah untuk terhapus, serta begitu seringnya menjalar keberbagai lokasi. Peraturan pada proses pengambilan serta retensi dari data menjadi sangat penting. Daripada itu, keahlian para pelaku dari kejahatan siber untuk menutupi jejak dari dihital mereka sendiri dengan penggunaan metode enskrpsi, biasa disebut dengan pemanfaatan fasilitas anonym, contohnya Dark Web serat VPN, yang menyebabkan semakin persulit proses pelacakan serta investigasi terhadap pembuktian kejahatan siber.sebagai contoh tantangan utama dalam penanganan kejahatan siber ini bahwasannya dalam pengumpulan, menganalisis serta mempresentasikan dari fakta digital yang bisa dterima pada proses peradilan.

Kemudian untuk tantangan selanjutnya yaitu ketersediaan dari sumber daya serta kemahiran dari para penegak hukum dalam menginvestigasi para penjahat siber dan juga dibutuhkan ilmu pengetahuan teknis dalam penanganannya lebih mendalam karena terkait terhadap sistem komputer, jaringannya serta pada metode forensic digitalnya, tetapi dalam hal ini tidak semua pada kelembagaaan penagakkan hukum telah memiliki personal dengan kemahiran yang akseptabel dalam penanganan bidang kejahatan siber ini. Dengan lemahnya dari tingkat pengetahuan personil dapat menyebabkan barang bukti dalam penanganan kasus kejahatan siber akan sangat lemah serta terjadinya ketidakmampuan dalam menganalisis bukti-bukti secara efesien.

Kemudian terhadap negara yang sedang berkembang tantangannya sering kali trjadinya kesenjangan kapasitas seperti berhubungan dengan pemenuhan dari infrastruktur teknologi serta pada sumber daya manusia dalam penanganan kejahatan siber secara berhasil. Selain itu terjadi perbedaan aturan hukum serta regulasi perundangan antara negara-negara tersebut dalm membentuk kerjasama dalam penegakkan hukum akan menjadi sangat sulit. Contohnya pada aktivitas yang diduga illegal pada sah sat negara api tiak diakui leh negara lainnya bawa itu sebagai suau pelanggaran. Tantangan berikutnya yaitu kenginan setiap negara yang berbada-beda dalam penanganan kejahatan sber n dan pada umumna ereka mempunya prioritas yan berbeda dalm penanganan keamanan siber, sehinga dengan hal ini meyebabkan terhambatnya kerjasama internasional. Banyak negara-negaa yang hanya berinti terhadap perlindungan serta keamanan daa pribadi, sedangkan untuk penanganan kejahatan siber pada negara lainnya juga hanya terfokus terhadap kemananan negaranya secara nasional.

Dari beragai tantangan-tantangan tersebut maka peluang dari ICC dalam penanganan kejahatan siber crime yaitu terdapat 3 pembagian peluang sebagai berikut;

1. Peningkatan kualitas dan kapasitas teknologi serta sumber daya manusia serta di dukung oleh ide-ide dari ICC terhadap negara-negara berkembang dalam penanganan kejahatan siber. Juga diperlukan saling memberikan informasi pengetahuan antara negara-negara maju juga dibutuhkan pada negara berkembang lainnya.
2. Sinkronisasi hukum dalam mengharmonisasikan peraturan perundangan serta regulasi terpaut kejahatan siber crime yang terjadi diberbagai negara dan juga dapat memudahkan kerjasama penegakan hukum lintas batasan. Dalam hal ini diperlukan suatu konvensi kerjasama internasional melalui perjanjian-perjanjian yang mengikat antar negara baik dari negara maju sampai negara berkembang yang semuanya itu tetap dalam kontrol ICC.
3. Pembuatan sistem alat serta mekanime penggunaan baru untuk mendukung pencegahan kejahatan siber internasional. Maka diperlukan pusat koordinasi internasional dalam tindakan nyata terhadap kejahatan siber sehingga membantu juga dalam penanggulangannya.

Untuk kejahatan siber ini sebenarnya sudah terdapat dalam konvensi Budapest. Konvensi ini merupakan sebagai kerangka hukum internasional ICC yang paling lengkap serta terakui secara meluas diseluruh negara internasional karena dalam menanggulangi terhadap kejahatan siber. Dalam konvensi Budapest juga memberikann pedman terhadap negara internasional untuk penegakkan hukum.

C. PENUTUP

Dari penjabaran pembahasan tersebut diatas penulis dapat menyimpulkan bahwa implementasi dasar hukum internasional untuk pelaksanaan penegakkan terhadap hukum kejahatan siber dan juga agresi siber crime sangat krusial dan kompleksitas. Perlu adanya kerjasama internasional, kedaulatan serta tidak adanya intervensi dari antar negara dalam penagulangan atau pencegahan dari kejahatan siber crime. ICC atau Mahkamah Pidana Internasional tidak dapat meiliki perundangan untuk melakukan penuntutan terhadap kejahatan siber crime, penyebab ICC tidak dapat melakkan penuntutan karena ICC mempunya prinsip bahwa hanya untuk kejahatan-kejahatan yang paling parah dan berhubungan dengan kemanusiaan langsung, seperti kejahatan terhadap peperangan, kejahatan terhadap kemanuasiaan, kejahatan terhadap genosida serta kejahatan terhadap agresi.

Penegakkan peraturan hukum yang harus dilakukan oleh Mahkamah Pidana Internasional atau ICC sangat penting untuk agresi kejahatan terhadap siber crime dan perlu secara konkret di laksanakan oleh seluruh negara internasional serta pelaksanaan konvensi Budapest. Konvensi ini merupakan sebagai kerangka hukum internasional terutama dalam penanggulangan kejahatan siber crime.

`

DAFTAR PUSTAKA

A. Farhan, R., Hidayat M., Syaefunaldi, D. R., & Hosnah, A. U.. Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber. Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora. Vol.1. No.6 (2023).

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A.. *Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia*. Justisia: Jurnal Ilmu Hukum. Vol.1. No.1 (2023).

Bambang S, Hartono, Hapsari, Rekka Ayu. *Mutual Legal Assistance terhadap pemberantasan Siber Crime Lintas Yurisdiksi di Indonesia*. Sasi. Vol.25. No.1 (2019).

Chotimah, H. C., Iswardhana, M. R., & Pratiwi, T. S. *Penerapan Military Confidence Building Measures dalam Menjaga Ketahanan Nasional Indonesia di Ruang Siber*. Jurnal Ketahanan Nasional. Vol.25. No.3 (2020).

Clought, Jonathant B. 2010. *Principles of The Cybercrime*. Cambridge: The Cambridge University Press.

Mustameer, H. *Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0*. Jurnal Yustika: Media Hukum Dan Keadilan. Vol.25. No.01 (2023).

Noor, Thalis. *Agresi serta Kejahatan terhadap Perdamaian*. Supremasi Hukum. Vol.3. No.1 (2014)

Najwa, R.. *Analisis Hukum terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia*. AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum. Vol.2. No.1 (2024).

Situmeang, M.. *Penyalahgunaan terhadap Data Pribadi sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber*. Sasi. Vol.27. No.1 (2022).

Schmit, R, Michael NS.. *Cyber In Operations the Jus in The Bello: Key In Issues.* The International In Law Studies. Vol. 90 (2014).