PAULUS Law Journal
Volume 5 Nomor 1, September 2023
e-ISSN : 2722-8525

PERAN INTELIJEN KEPOLISIAN SEBAGAI TINDAKAN PREVENTIF DALAM MENANGGULANGI TINDAK PIDANA CYBER CRIME

Pramawi Nicolas Huliselan
Magister Ilmu Hukum Universitas Kristen Indonesia Paulus, framawi24@gmail.com

Abstrak
Intelijen Kepolisian merupakan salah satu bidang dalam tubuh Kepolisian Republik Indonesia yang memiliki fungsi sebagai mata dan telinga bagi organisasi Kepolisian dalam mencegah dan menanggulangi tindak pidana *cyber crime*. Tujuan penelitian ini adalah untuk menganalisis peran Intelijen Kepolisian dalam melakukan deteksi dini terjadinya tindak pidana *cyber crime* dan untuk mengetahui kendala-kendala yang dihadapi Intelijen Kepolisian dalam menanggulangi tindak pidana *cyber crime*. Penelitian ini menggunakan tipe penelitian normatif empiris, dengan menggunakan data primer dan data sekunder. Data primer diperoleh langsung dari penelitian di lapangan, sedangkan data sekunder terdiri dari bahan hukum primer dan bahan hukum sekunder. Hasil penelitian menunjukkan bahwa peran intelkam dalam mencegah terjadinya tindak pidana *Cyber Crime* terdiri dari peran normatif dan peran faktual. Peran normatif dilaksanakan berdasarkan ketentuan dalam peraturan perundang-undangan, dimana dalam hal ini intelkam berperan sesuai dengan peraturan perundang-undangan yang terkait dengan tindak pidana *Cyber Crime*. Sedangkan peran faktual dilaksanakan oleh Intelkam Kepolisian dalam penanggulangan tindak pidana *cyber crime* dengan berdasar pada fakta ancaman yang terjadi dalam kehidupan masyarakat. Adapun kendala-kendala yang dihadapi oleh Intelkam dalam mencegah tindak pidana *cyber crime* yaitu faktor sumber daya manusia dan sarana prasarana.
Kata Kunci : Peran; Intelijen Kepolisian; Cyber Crime

Abstract
Police Intelligence is a sector within the Indonesian National Police which functions as the eyes and ears of the Police organization in preventing and dealing with cyber crimes. The aim of this research is to analyze the role of Police Intelligence in carrying out early detection of cyber crime and to determine the obstacles faced by Police Intelligence in tackling cyber crime. This research uses an empirical normative research type, using primary data and secondary data. Primary data is obtained directly from research in the field, while secondary data consists of primary legal materials and secondary legal materials. The research results show that the role of intelligence and security in preventing the occurrence of Cyber Crime crimes consists of a normative role and a factual role. The normative role is carried out based on provisions in statutory regulations, where in this case intelligence and security play a role in accordance with statutory regulations related to Cyber Crime crimes. Meanwhile, the factual role is carried out by Police Intelligence and Security in dealing with cyber crimes based on the facts of threats that occur in people's lives. The obstacles faced by Intelkam in preventing cyber crime include human resources and infrastructure.
Keywords : Role; Police Intelligence; Cyber Crime

I. PENDAHULUAN

Dalam mengatur kehidupan bermasyarakat, hukum menjadi sarana kontrol sosial. Salah satu perwujudan hukum sebagai sarana kontrol sosial adalah dengan adanya pemidanaan, di mana di dalamnya terdapat larangan, yang ketika dilanggar

maka akan dikenakan sanksi negatif bagi pelanggarnya.[1] Hukum menetapkan apa yang harus dilakukan dan atau apa yang tidak boleh dilakukan.

Achmad Ali menyatakan bahwa hukum merupakan seperangkat kaidah atau aturan yang tersusun dalam suatu sistem yang menentukan apa yang boleh dan tidak boleh dilakukan oleh manusia sebagai warga dalam kehidupan bermasyarakat. Hukum tersebut bersumber dari masyarakat sendiri maupun dari sumber lain yang diakui berlakunya oleh otoritas tertinggi dalam masyarakat tersebut, serta diberlakukan oleh warga masyarakat (sebagai satu keseluruhan) dalam kehidupannya.[2] Apabila terdapat pelanggaran atas kaidah tersebut, maka akan memberikan kewenangan bagi otoritas tertinggi untuk menjatuhkan sanksi yang sifatnya eksternal.

Perkembangan teknologi komunikasi telah membawa perubahan besar terhadap sendi kehidupan manusia. Tidak dapat dipungkiri bahwa perkembangan teknologi telah memberikan dampak positif terhadap kemajuan manusia hidup manusia suatu bangsa. Perkembangan teknologi komputer dan internet misalnya, telah memberikan banyak kemudahan bagi manusia dalam menjalankan aktivitasnya, tidak hanya dalam berkomunikasi melainkan berbagai transaksi, kapanpun dan dimana pun.[3] Teknologi komunikasi telah membuat jarak dan waktu menjadi tidak terbatas, di mana orang dapat melakukan berbagai aktivitas yang pada dasarnya sulit dilakukan dalam dunia nyata menjadi lebih mudah.

Hukum memiliki tujuan sebagai alat rekayasa sosial. Dalam hal ini, perkembangan teknologi yang begitu pesat perlu diatur sedemikian rupa agar tetap dapat dipergunakan dalam koridor yang sebagaimana mestinya. Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) menjadi dasar hukum bagi masyarakat dalam memanfaatkan perkembangan teknologi. Dalam Pasal 3 UU ITE disebutkan bahwa pemanfaatan teknologi informasi dan transaksi elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi. Adapun tujuan dari pemanfaatan teknologi sebagaimana diatur dalam Pasal 4 UU ITE, yaitu :

1. Mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia.
2. Mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat.
3. Meningkatkan efektivitas dan efisiensi pelayanan publik.

[1] Zainuddin Ali, 2019, *Sosiologi Hukum*, Sinar Grafika, Jakarta, hlm. 22
[2] Achmad Ali, 2011, *Menguak Tabir Hukum*. Ghalia Indonesia, Bogor, hlm. 30-31
[3] Abdul *Wahid* dan Mohammad *Labib*, 2010, *Kejahatan Mayantara*. Refika Aditama, Bandung, hlm. 24

4. Membuka kesempatan seluas-luasnya kepada setiap Orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan teknologi Informasi seoptimal mungkin dan bertanggung jawab.
5. Memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara teknologi Informasi.

Meskipun telah diatur sedemikian rupa dalam UU ITE, dalam perkembangannya terdapat dampak negatif yang dapat ditimbulkan dari perkembangan teknologi informasi dan komunikasi. Dalam hal ini, perkembangan teknologi dapat dimanfaatkan sebagai sarana untuk melakukan kejahatan. Salah satu bentuk kejahatan yang menggunakan perkembangan teknologi informasi dan komunikasi adalah kejahatan siber atau yang lazim disebut dengan *cyber crime*. *Cyber crime* merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya *(cyberspace)* dan tindakan kejahatan yang menggunakan komputer.[4] Menurut Freddy Haris, *cyber crime* memiliki karakteristik, yaitu:[5]

1. *Unauthorized access.*
2. *Unauthorized alteration or destruction of data.*
3. Mengganggu atau merusak operasi komputer
4. Mencegah atau menghambat akses pada komputer.

Begitu maraknya kasus *cybercrime* yang terjadi dewasa ini, membuat isu mengenai *cyber crime* menjadi pembahasan yang sangat mengemuka di berbagai negara, tidak terkecuali Indonesia. Pada umumnya, bentuk *cyber crime* yang dikenal dalam masyarakat dapat dibedakan dalam tiga kualifikasi, yaitu :[6]

1. Kejahatan dunia maya yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer.
2. Kejahatan dunia maya yang menggunakan komputer sebagai alat kejahatan.
3. Kejahatan dunia maya yang berkaitan dengan isi atau muatan data atau sistem komputer.

Di Indonesia, *cyber crime* tercatat telah terjadi sejak tahun 1983 terutama di bidang perbankan. Dalam perkembangannya hingga saat ini, jenis *cyber crime* yang marak terjadi di Indonesia adalah pembajakan program komputer, *cracking*, penggunaan kartu kredit pihak lain secara tidak sah *(carding)*, *pembobolan bank (banking fraud)*, pornografi, termasuk kejahatan terhadap nama domain *(domain name)*, dan penyebaran berita bohong *(hoax)*.

Wakil Kepala Kepolisian Republik Indonesia tahun 2018, Komisaris Jendral Syafruddin pernah menyatakan bahwa Indonesia masuk dalam jajaran dua besar

[4] Didik M. Arief Mansur dan Elisatris Gultom, 2005**,** *Cyber Law: Aspek Hukum Teknologi Informasi,* Refka Aditama, Bandung, hlm. 19

[5] Lita Sari Marita, 2015, *Cyber Crime dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law di Indonesia*, Jurnal Cakrawala Vol. 15 No. 2, hlm. 2

[6] Muhammad Anthony Aldriano, Mas Agus Priyambodo, 2022, *Cyber Crime Dalam Sudut Pandang Hukum Pidana*, Jurnal Kewarganegaraan Vol. 6 No. 1, hlm. 2170

negara di dunia dengan kejahatan dunia maya. Selama bulan Januari hingga akhir Juni tahun 2016, pihak Kepolisian mendapati sebanyak 90 juta kali serangan siber terjadi di Indonesia.[7] Data dari Baresrkim Polri sejak tahun 2015 mencatat terdapat sebanyak 100.000 akun di media sosial yang menyebarkan *hate speech*. Di samping itu, ancaman terorisme global juga semkain bergerak melalui sarana dunia maya dalam melakukan strategi. Banyaknya kasus dan besarnya potensi ancaman kerugian yang ditimbulkan dari *cyber crime* ini membuat pemerintah Indonesia memberikan perhatian yang sangat besar terhadap kejahatan ini.

Untuk melindungi kepentingan masyarakat terhadap penyalahgunaan teknologi, pada dasarnya pemerintah telah memberi jaminan perlindungan terhadap kepentingan masyarakat. Pasal 40 ayat (2) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyebutkan bahwa Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan peraturan perundang-undangan.

Polri merupakan salah satu aparat penegak hukum dalam sistem peradilan pidana yang memiliki peran sebagai pelopor, stabilisator dan dinamisator dalam pembangunan nasional dalam rangka pencapaian tujuan nasional. G Gewin menyatakan, bahwa tugas Polisi merupakan bagian dari tugas negara, perundang-undangan dan pelaksanaan untuk memberi jaminan tata tertib ketenteraman dan keamanan negara, menanamkan ketaatan dan kepatuhan. Dalam konteks sistem ketatanegaraan, lembaga Kepolisian merupakan lembaga tinggi yang bersifat non departemen sebagaimana halnya lembaga Kejaksaan Agung.[8] Terkait dengan sistem hukum pidana, Kepolisian merupakan garda terdepan, di mana proses dalam sistem peradilan pidana di Indonesia diawali di tingkat Kepolisian, sehingga Kepolisian juga sering disebut sebagai hukum pidana yang hidup.

Semakin berkembangnya dunia kriminalitas dengan memanfaatkan perkembangan teknologi membuat lembaga Kepolisian juga harus bergerak dinamis dalam mengikuti perkembangan zaman. Salah satu bidang dalam Lembaga Kepolisian yang terkait dengan kejahatan tersebut adalah bidang Intelijen dan Keamanan (Intelkam) yang dapat menjadi pintu dalam membantu dalam pemberantasan tindak pidana *cyber crime*.

Dalam Pasal 1 angka 2 Peraturan Kepala Badan Intelijen Keamanan Kepolisian Republik Indonesia Nomor 4 Tahun 2012 tentang Pertelaan Tugas di Lingkungan Badan Intelijen Keamanan Kepolisian Negara Republik Indonesia

---

[7] *Polri: Indonesia Tertinggi Kedua Kejahatan Siber di Dunia*, dalam website https://www.kominfo.go.id/content/detail/13487/polri-indonesia-terfinggi-kedua-kejahatan-siber-di-dunia/0/sorotan_media, diakses tanggal 2 Maret 2023

[8] Ketut Adi Purnama, 2018, *Hukum Kepolisian Sejarah dan Peran POLRI Dalam Penegakan Hukum serta Perlindungan HAM,* Refika Aditama, Bandung, hlm. 36.

disebutkan bahwa intelijen merupakan usaha dan/atau kegiatan yang terorganisir dengan menggunakan metode tertentu untuk menghasilkan produk berupa pengetahuan mengenai masalah yang dihadapi, kemudian disajikan kepada pimpinan sebagai bahan pengambilan keputusan dan tindakan atau perumusan kebijaksanaan. Pemaknaan intelijen pada dasarnya dapat dibedakan sebagai bahan keterangan yang sudah diolah, sebagai suatu organisasi, dan sebagai kegiatan.

Keberadaan Intelkam Polri sangat penting dalam memberikan masukan kepada pimpinan mengenai perkembangan situasi dan kondisi kamtibmas. Dalam hal ini, diperlukan data dan analisa yang akurat sehingga segala kemungkinan ancaman dapat diantisipasi dengan baik. Terkait dengan *cyber crime*, Intelkam menjadi mata dan telinga untuk melakukan deteksi dini sekaligus menjadi *early warning* ketika terdapat ancaman terhadap penyalahgunaan teknologi informasi dan komunikasi. Dalam berbagai kasus mengenai *cyber crime*, keberadaan intelkam digunakan sebagai bagian dari penegakan hukum matau *law enforcement*. Dengan kata lain, fungsi intelkam lebih banyak dilaksanakan ketika telah terjadi kejahatan siber. Jika dilihat lebih luas, sama seperti fungsi lembaga Kepolisian pada umumnya, fungsi intelkam tidak hanya dalam rangka penegakan hukum semata, melainkan juga pada tindakan preventif. Dalam hal ini, diperlukan optimalisasi peran intelkam tidak hanya dalam hal penegakan hukum terhadap *cyber crime*, melainkan juga mencegah terjadinya tindak pidana *cyber crime*.

II. Kepolisian Negara Republik Indonesia

1. Pengertian Kepolisian

Lembaga kepolisian memiliki peran yang sangat besar dalam rangka menjaga keamanan sekaligus melindungi negara. Dari sudut pandang kesejarahan dan etimologi, pada awalnya istilah 'Polisi berasal dari bahasa Yunani, yaitu "Politeia" yang berarti seluruh pemerintah negara kota. Pada abad sebelum masehi, negara Yunani terdiri dari kota-kota yang dinamai "Polis" yang memiliki ari luas, yaitu pemerintahan yang meliputi seluruh pemerintahan kota termasuk urusan keagamaan atau penyembahan terhadap dewa-dewa. Keberadaan agama Nasrani kemudian membawa perubahan pada pemaknaan kata "Polis", dimana kata tersebut diartikan sebagai seluruh pemerintahan, yang di dalamnya tidak termasuk urusan keagamaan.[9] Dalam perkembangannya, Polisi mengandung arti sebagai organ dan fungsi, yakni sebagai organ pemerintah yang memiliki tugas mengawasi, jika perlu menggunakan paksaan agar masyarakat tidak melakukan larangan-larangan.

Berdasarkan Kamus Besar Bahasa Indonesia (KBBI), arti kata polisi adalah suatu badan yang bertugas memelihara keamanan dan ketentraman dan ketertiban umum (menangkap orang yang melanggar hukum), merupakan suatu anggota

[9] Momo Kelana, 1984, *Hukum Kepolisian,* Edisi ketiga, PTIK, Jakarta, hlm. 15.

badan pemerintah (pegawai negara yang bertugas menjaga keamanan dan ketertiban). Di Indonesia, Kepolisian sebagai subsistem peradilan pidana diatur dalam Undang-undang Nomor. 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia. Dalam Pasal 1 angka 1 Undang-Undang Kepolisian Negara Republik Indonesia, disebutkan bahwa Kepolisian merupakan segala hal ihwal yang berkaitan dengan fungsi dan lembaga polisi sesuai dengan peraturan perundang-undangan. Berdasarkan pengertian tersebut, Kepolisian mengandung dua pengertian, yaitu sebagai fungsi dan sebagai lembaga.

Kepolisian sebagai sebuah fungsi yaitu sebagai salah satu fungsi pemerintahan negara di bidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, pelindung, pengayom dan pelayan kepada masyarakat. Terkait dengan hal tersebut, segala tugas, wewenang serta tanggung jawab diberikan atas dasar undang-undang. Sedangkan lembaga kepolisian adalah organ pemerintah yang ditetapkan sebagai suatu lembaga dan diberikan kewenangan menjalankan fungsinya berdasarkan peraturan perundang-undangan.[10] Sebagai sebuah organ, Kepolisian merupakan suatu lembaga yang terorganisasi dan terstruktur dalam organisasi negara.

Dari hal tersbut dapat pula dibedakan pengertian kepolisian dalam arti formil dan dalam arti materil. Dalam arti formil, mencakup penjelasan mengenai organisasi dan kedudukan dalam instansi kepolisian. Sedangkan kepolisian dalam arti materiil mencakup tugas dan wewenang dalam menghadapi gangguan keamanan dan ketertiban, baik dalam kewenangan kepolisian umum maupun ketentuan-ketentuan yang diatur dalam peraturan undang-undang kepolisian secara khusus.

Berdasarkan Pasal 2 Undang-Undang Kepolisian Negara Republik Indonesia, fungsi Kepolisian merupakan bagian dari fungsi pemerintahan negara di bidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan, pengayoman dan pelayanan kepada masyarakat. Untuk itulah, Kepolisian bertujuan untuk mewujudkan keamanan dalam negeri yang meliputi terpeliharanya keamanan dan ketertiban masyarakat, tertib dan tegaknya hukum, terselenggaranya perlindungan, pengayoman dan pelayanan kepada masyarakat serta terbinanya ketenteraman masyarakat dengan menjunjung tinggi hak asasi manusia.

Tugas pokok tersebut diperinci dalam rumusan tugas-tugas yang susunannya mengacu pada susunan rumusan tugas pokok yang memuat tiga substansi yaitu :[11]

a. Substansi Tugas Pokok Memelihara dan Ketertiban masyarakat bersumber dari kewajiban umum kepolisian untuk menjamin keamanan umum.

[10] Sadjijono, 2006, *Hukum kepolisian, Perspektif Kedudukan dan Hubungan Dalam Hukum Administratif*, Laksbang PRESSindo, Yogyakarta, hlm. 40.

[11] H. Pudi Rahardi, 2007, *Hukum Kepolisian (Profesionalisme dan Reformasi Polri)*, Penerbit Laksbang Mediatama, Surabaya, hlm. 67-68

b. Substansi Tugas Pokok Menegakan Hukum bersumber dari ketentuan peraturan perundang-undangan yang memuat tugas pokok polri dalam kaitannya dengan peradilan pidana.
c. Substansi Tugas Pokok Polri untuk memberikan perlindungan, pengayoman dan pelayanan kepada masyarakat bersumber dari kedudukan dan fungsi kepolisian sebagai bagian dari fungsi pemerintahan negara yang pada hakekatnya bersifat pelayanan publik yang termasuk dalam kewajiban umum kepolisian.

Dalam pelaksanaan fungsi sebagai penegak hukum, polisi dituntut untuk memahami asas-asas yang selalu mendasari polisi dalam bertindak. Adapun asas-asas tersebut, yaitu :[12]

a. Asas Legalitas, dalam melaksankan tugasnya sebgai penegak hukum wajib tunduk pada hukum.
b. Asas Kewajiban, merupakan kewajiban polisi dalam menangani permasalahan masyarakat.
c. Asas Partisipasi, dalam rangka mengamankan lingkungan masyarakat polisi mengkoordinasikan pengamanan Swakarsa untuk mewujudkan ketaatan hukum di kalangan masyarakat.
d. Asas Preventif, selalu menedepankan tindakan pencegahan dari pada penindakan (represif) kepada masyarakat.
e. Asas Subsidiaritas, melakukan tugas instansi lain agar tidak menimbulkan permasalahan yaang lebih besar.

2. Intelijen Keamanan Kepolisian Negara Republik Indonesia

Dalam rangka pelaksanaan tugas-tugas intelijen di lingkungan Polri, kegiatan operasional Intelkam diklasifikasikan dalam tiga bentuk yang berlaku secara umum yaitu penyelidikan, pengamanan, dan penggalangan. Kegiatan operasional Intelkam dilakukan dengan tujuan untuk memperoleh informasi, mengamankan obyek/aktivitas tertentu, serta menciptakan kondisi yang kondusif bagi pelaksanaan tugas Polri lainnya, di mana kegiatan tersebut dapat dilakukan dalam bentuk operasi tertutup maupun operasi terbuka. Penyelidikan merupakan upaya mencari dan mengumpulkan bahan informasi. Pengamanan merupakan upaya mengamankan organisasi agar tidak menjadi sasasaran lawan. Sedangkan penggalangan merupakan upaya untuk menciptakan kondisi dan situasi yang menguntungkan organisasi. Oleh karena itu, spektrum kegiatan Intelkam dalam pelaksanaan tugas Polri adalah mendahului, menyertai dan mengakhiri setiap kegiatan operasional kepolisian yang dilakukan oleh Polri.[13]

[12] Bisri Ilham, 1998, *Sistem Hukum Indonesia*, Grafindo Persada, Jakarta, hlm.32
[13] Ary Purwanti, Burham Pranawa, Purwadi, 2021, *Deteksi Dini Oleh Intelkam Polri Dalam Mengantisipasi Gangguan Kamtibmas Pada Pilkada di Boyolali*, Jurnal Bedah Hukum, Vol. 5 No.1, hlm. 8

Dalam menjalankan fungsi penyelidikan, Intelkam mencari, mengumpulkan, mengolah data (bahan keterangan) dan menyajikan informasi sebagai bentuk penginderaan dan peringatan dini bagi pimpinan Polri, baik dalam bidang pembinaan maupun operasional kepolisian. Informasi serta data yang diperoleh harus selengkap mungkin dari berbagai sumber, baik itu sumber terbuka maupun tertutup melalui kegiatan yang juga terbuka maupun tertutup. Informasi serta data tersebut kemudian diolah menjadi produk intelijen yaitu informasi yang siap digunakan sebagai dasar pengambilan keputusan atau tindakan.

Terkait fungsi pengamanan, tugas intelkman ditujukan untuk mendukung penyelenggaraan tugas pokok Polri yang dilaksanakan dengan menerapkan prosedur, metode, tehnik dan taktik berupa langkah-langkah pencegahan dan penindakan baik langsung, terbuka ataupun tertutup yang terhadap segala bentuk ancaman yang mungkin terjadi berupa penyimpangan norma-norma untuk menjamin keamanan dan ketertiban dalam kehidupan, serta yang dapat diperkirakan akan menghambat kelancaran pelaksanaan pembangunan nasional. Pengamanan adalah upaya, langkah, dan tindakan yang dilakukan dengan tujuan untuk mangamankan suatu lingkungan beserta dengan segala isinya agar tercipta suasana aman dan tertib serta mensterilkan dari segala bentuk ancaman, gangguan, hambatan dan tantangan.[14]

Berdasarkan nomenklatur, Intelijen Keamanan (Intelkam) Polri mempunyai tugas untuk membina dan menyelenggarakan fungsi intelijen dalam bidang keamanan bagi kepentingan pelaksanaan tugas operasional dan manajemen Polri maupun guna mendukung pelaksanaan tugas-tugas pemerintahan dalam rangka mewujudkan keamanan dalam negeri. Intelijen dan keamanan (intelkam) Polri berkewajiban melaksanakan deteksi dini dan memberikan peringatan terhadap masalah dan perkembangan masalah serta perubahan kehidupan sosial dalam masyarakat.

Selain itu, intelkam dapat mengidentifikasi ancaman, gangguan, atau hambatan terhadap situasi keamanan dan ketertiban masyarakat.[15] Dengan demikian, intelkam dapat disebut sebagai garda terdepan Polri dalam mengayomi masyarakat dan menangkal segala sesuatu yang dapat mengganggu ketertiban dan keamanan. Terkait dengan tugas Intelkam, dibagi berdasarkan tingkat kewilayahan, mulai dari Markas Besar, Kepolisian Daerah (Polda), Kepolisian Resor (Polres), hingga Kepolisian Sektor (Polres).

Pada tingkat Markas Besar Polri disebut dengan Badan Intelijen Keamanan (Baintelkam) Polri yang bertugas membantu Kapolri dalam membina dan menyelenggarakan fungsi intelijen keamanan bagi kepentingan pelaksanaan tugas dan menajemen Polri secara umum guna mendukung pelaksanaan tugas-tugas

[14] Ibid, hlm. 9

[15] Tim Penyusun, 2012, *Naskah Pencerahan Intelkam*, Baintelkam Polri, Jakarta, hlm 35

pemerintahan dalam rangka mewujudkan keamanan dalam negeri. Di tingkat Polda, Intelkam Polri disebut Direktorat Intelijen Kemanan (Ditintelkam) yang merupakan unsur pelaksana tugas pokok dalam bidang intelijen keamanan pada tingkat Polda yang berada di bawah Kapolda. Adapun tugas Ditintelkam yaitu :

a. Melakukan deteksi aksi intelijen berupa deteksi dini, peringatan dini dan/atau cegah dini dengan didukung teknologi intelijen dan persandian.
b. Memberikan pelayanan administrasi dan pengawasan senjata api atau bahan peledak, orang asing, dan kegiatan sosial atau politik masyarakat sesuai dengan ketentuan peraturan perundang-undangan.
c. Mengumpulkan, mengolah dan mendokumentasikan data serta menyajikan informasi kepada pimpinan, satuan fungsi kepolisian dan instansi terkait.

Di tingkat Polsek, keberadaan Intelkam disebut dengan Unit Intelijen Keamanan (Unit Intelkam) yang bertugas menyelenggarakan fungsi intelijen keamanan meliputi pengumpulan bahan keterangan/informasi untuk keperluan deteksi dini dan peringatan dini, dalam rangka pencegahan terjadinya gangguan keamanan dan ketertiban masyarakat, serta pelayanan perizinan sesuai kewenangannya.

Perkembangan kehidupan masyarakat yang bergerak secara dinamis memiliki konsekuensi pula pada perkembangan situasi kamtibmas. Di satu sisi pembangunan nasional membutuhkan situasi kamtibmas yang kondusif, sehingga peran serta keberadaan Intelkam sangat penting. Dalam hal ini ini, peran Intelkam harus dapat mengantisipasi berbagai perkembangan situasi sehingga apabila muncul ancaman faktual dapat ditangani secara profesional dan proporsional sesuai dengan prosedur yang ditetapkan dalam peraturan perundang-undangan. Peran Intelkam Polri dapat menjadi penghubung dan penjaga dinamika sosial yang berkembang dalam masyarakat terkhusus dalam konsep masyarakat.

Intelkam memberikan peringatan dini kepada pengambil kebijakan, sehingga menjadi suatu hal yang mutlak ketika Intelkam harus meningkatkan kualitas informasi dan data yang diberikan dalam produk tertulis dari kegiatan intelijen khususnya dengan pemutakhiran serta korelasi dengan fenomena situasi yang sering terjadi. Fungsi Intelkam sangat berperan dalam memberikan masukan kepada pimpinan tentang perkembangan keamanan dan ketertiban dalam masyarakat. Intelkam merupakan garda terdepan dalam menyikapi dinamika sosial yang berkembang terutama hal-hal vital sekarang ini seperti tentang agama, ekonomi, dan budaya. Oleh karenanya, diperlukan analisa Intelkam yang tajam dan akurat sehingga segala kemungkinan tentang perkembangan kamtibmas dapat diantisipasi oleh kepolisian. Maka dituntut peran dan fungsi intelkam untuk menjalankan tugasnya menghadapi perkembangan paradigma kamtibmas yang terjadi di wilayah tugasnya masing-masing.

3. Tinjauan Mengenai *Cyber Crime*

Perkembangan teknologi informasi komunikasi sebagai salah satu bagian dalam era globalisasi telah membawa dunia menjadi semakin transparan dan bahkan menjadi dunia tanpa batas yang kemudian menciptakan struktur global yang baru. Hal ini jelas membawa dampak pada perubahan sosial yang berlangsung demikian cepat. Dalam hal ini, perubahan yang terjadi bagai pisau bermata dua, dimana perubahan tersebut tidak saja memberikan dampak positif, melainkan juga dampak negatif. Perkembangan teknologi informasi komunikasi dapat memberikan kontribusi bagi peningkatan kesejahteraan dan peradaban manusia. Namun, di sisi lain, hal ini juga menjadi sarana bagi manusia untuk melukan perbuatan melawan atau melanggar hukum.

Salah satu dampak negatif yang muncul akibat perkembangan tekologi informasi adalah lahirnya kejahatan-kejahatan yang sifatnya baru khususnya yang memanfaatkan sarana internet sebagai alat bantunya yang disebut juga *cyber crime* atau kejahatan di dalam dunia maya, seperti *hacker, cracker, cybersquating*, dan sebagainya. Setiap orang yang menguasai dan mempu mengoperasikan komputer memiliki potensi untuk melakukan kejahatan ini, di mana *cyber crime* dilakukan dengan merusak data, mencuri data, dan menggunakannya secara illegal.[16] Kejahatan ini dapat dilakukan oleh seseorang maupun secara berkelompok.

Dari sudut pandang kesejarahan, *cyber crime* pertama kali terjadi di Amerika Serikat pada tahun 1960-an. Pada tahun 1970 di Amerika Serikat terjadi kasus manipulasi data nilai akademik mahasiswa di Brooklyn College New York, kasus penyalahgunaan komputer perusahaan untuk kepentingan karyawan, kasus pengkopian data untuk sarana kejahatan penyelundupan narkotika, dan kasus penipuan melalui kartu kredit. Selain itu terjadi pula kasus akses tidak sah terhadap database *security pacific national bank* yang mengakibatkan kerugian sebesar $10.2 juta US pada tahun 1978. Kejahatan serupa juga terjadi di sejumlah negara antara lain Jerman, Australia, Inggris, Finlandia, Swedia, Austria, Jepang, Kanada, Belanda, dan Indonesia, di mana kejahatan tersebut menyerang terhadap harta kekayaan, kehormatan sisitem dan jaringan komputer.[17]

Cyber crime sering disebut sebagai bentuk kejahatan yang ditimbulkan melalui pemanfaatan teknologi internet. Forester dan Morrison, pakar komputer asal Amerika Serikat menggambarkan bahwa kejahatan komputer merupakan suatu tindak kriminal di mana alat atau senjata yang digunakan untuk melakukan kejahatan tersebut adalah komputer. Seorang pakar lainnya, Eoghan Casey menyatakan bahwa *cyber crime* merupakan suatu terminologi yang dipakai untuk mendeskripsikan aktivitas kejahatan yang menggunakan komputer atau jaringan

[16] H.Sutarman, 2007, *Cyber Crime - Modus Operandi dan Penanggulangannya*, Laksbang Pressindo, Yogyakarta, hlm. 4

[17] Sri Sumarwani, 2014, *Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif*, Jurnal Pembaharuan Hukum, Vol. 1 No. 3, hlm. 289

sebagai alat atau senjata sasaran kejahatan tersebut atau sebagai tempat terjadinya kejahatan. Karena banyak berhubungan dengan komputer, *cyber crime* sering atau identik dengan *computer crime*. *Cybercrime* menurut The U.S. Dept.of Justice, *computer crime* adalah indakan ilegal apapun yg memerlukan pengetahuan tentang teknologi komputer untuk perbuatan jahat, penyidikan, atau penuntutan.

Meskipun belum terdapat kesepahaman mengenai definisi *cyber crime* namun pada dasarnya terdapat kesepahaman dalam mendefinisikannya yaitu upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa izin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut. Pada dasarnya *cyber crime* meliputi semua tindak pidana yang terkait dengan informasi, sistem informasi itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian atau pertukaran informasi itu kepada pihak lainnya.

Dengan mengandalkan perkembangan teknologi informasi komunikasi, *cyber crime* dapat dilakukan tanpa memerlukan adanya kontak langsung antara pelaku dengan korban. Kejahatan ini dapat dilakukan dimana saja, tanpa memperhitungkan jarak antara pelaku dengan target kejahatan, sepanjang terdapat jaringan internet dan peralatan yang memadai. Roderic Broadhurst, Peter Grabosky, Mamoun Alazab dan Steve Chon menyatakan bahwa pelaku *cyber crime* dapat beroperasi sebagai jaringan longgar, namun bukti menunjukkan bahwa anggota masih berada dalam jarak yang dekat bahkan serangan mereka dapat melintasi negara.[18]

Begitu maraknya perkembangan kejahatan dunia maya ini bahkan mendapat perhatian besar oleh dunia internasional. *European Convention on Cybercrime November 23th 2001* di Hongaria atau yang dikenal dengan *Budapest Convention* telah dibentuk oleh masyarakat internasional dengan kenyataan adanya karakteristik ancaman siber yang bersifat tanpa batas dan menggunakan teknologi tinggi sebagai medianya. Kovensi ini melihat kebijakan kriminalisasi di bidang teknologi informasi yang harus memperhatikan perkembangan upaya penanggulangan *cybercrime* baik regional maupun internasional dalam rangka harmonisasi dan uniformitas pengaturan *cyber crime*.[19]

Dalam *Budapest Convention*, terdapat tiga jenis kategori ancaman yang dapat ditimbulkan oleh *cyber crime*, yaitu :[20]

a. Kategori pertama, yaitu kumpulan jenis serangan dimana teknologi informasi dan komunikasi menjadi alat atau senjata utama untuk melakukan kejahatan. Contohnya adalah komputer dan internet dipergunakan sebagai alat dan sarana untuk menyebarkan aliran-aliran sesat, telepon genggam yang digunakan untuk

[18] Dewi Bunga, 2019, *Politik Hukum Pidana Terhadap Penanggulangan Cyber Crime*, Jurnal Legislasi Indonesia, Vol. 16 No. 1, hlm. 2

[19] Yosua Praditya Suratman, 2017, *Penggunaan Strategi Operasi Kontra Intelijen Dalam Rangka Mengahadapi Ancaman Siber Nasiona*l, Jurnal Pertahanan dan Bela Negara, Vol. 7 No. 2, hlm. 4

[20] Ibid, hlm. 5

mengirimkan pesan-pesan untuk menipu calon korban, dan *electronic mail* yang digunakan sebagai sarana untuk mengirimkan gambar-gambar atau video bernuansa pornografi.

b. Kategori Kedua, yaitu komputer atau teknologi informasi menjadi sasaran pusat serangan dari pelaku tindak kejahatan, seperti melakukan transaksi keuangan fiktif dalam sebuah sistem perbankan berbasis internet (*e-banking),* mematikan atau memacetkan kerja-kerja sebuah jejaring internet secara remote, dan menyebarkan virus-virus untuk mengganggu kinerja komputer-komputer tertentu.
c. Kategori ketiga, yaitu ancaman siber yang ditujukan bagi peristiwa yang bertujuan merusak data atau informasi tersimpan dalam media perangkat teknologi informasi. Serangan pada kategori ini dapat berupa merubah isi sebuah situs tanpa sepengetahuan pemiliknya, mengambil kumpulan *password* atau informasi lengkap kartu kredit sekelompok individu untuk disalahgunakan atau diperjualbelikan, dan merusak sistem basis data utama sehingga informasi di dalamnya menjadi tidak dapat terbaca atau diakses secaa normal dan lain sebagainya.

Dari ketiga kategori ancaman tersebut menunjukan bahwa subjek ancaman *cyber crime* tidak hanya ditujukan kepada pemerintah, tetapi juga termasuk individu, kelompok masyarakat, dan perusahaan.

Mcdonnell dan Sayers berpendapat bahwa, ancaman siber terdiri atas tiga jenis, yaitu:[21]

a. Ancaman perangkat keras (*hardware threat*)
   Merupakan ancaman yang disebabkan oleh pemasangan perangkat tertentu yang berfungsi untuk melakukan kegiatan tertentu didalam suatu sistem, sehingga peralatan tersebut merupakan gangguan terhadap sistem jaringan dan perangkat keras lainnya.
b. Ancaman perangkat lunak (*software threat)*
   Merupakan ancaman yang disebabkan masuknya perangkat lunak tertentu yangberfungsi untuk melakukan kegiatan pencurian, perusakan, dan manipulasi informasi.
c. Ancaman data/informasi (*data/information threat)*
   Merupakan ancaman yang diakibatkan oleh penyebaran data/informasi tertentu yang bertujuan untuk kepentingan tertentu.

Sebagai sebuah kejahatan dengan gaya baru, *cyber crime* bukanlah kejahatan sederhana karena tidak lagi menggunakan sarana konvensional melainkan menggunakan komputer dan internet. *Cyber crime* dapat pula disebut sebagai kejahatan yang berkorelasi dengan kepentingan seseorang atau sekelompok orang,

[21] Ineu Rahmawati, 2017, *Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defence*, Jurnal Pertahanan dan Bela Negara, Vol. 7 No. 2, hlm. 55

baik yang memanfaatkan atau dimanfaatkan untuk memperluas daya jangkauan *cyber crime*.[22] Banyak motif yang melandasi seseorang atau kelompok untuk melakukan kejahata ini, diantaranya kepentingan bisnis, politik, budaya, ekonomi, dan sebagainya. Meskipun merupakan kejahatan dunia maya, bukan berarti kejahatan ini tidak menimbulkan korban. Bahkan, pihak yang menjadi korban berlapis-lapis baik secara privat maupun publik dan terus berkembang dari hari ke hari.

Cyber crime umumnya dilakukan dengan tujuan untuk menghasilkan keuntungan finansial bagi pelakunya. Adapula pelaku yang menggunakan internet sebagai media untuk menghasilkan uang, misalnya penggunaan internet untuk perdagangan gelap senjata, prostitusi dan pornografi. Selain itu, dalam perkembangannya, media internet juga digunakan sebagai sarana untuk menyerang pribadi seseorang tanpa secara langsung atau memang tidak bertujuan untuk keuntungan finansial, misalnya pencemaran nama baik melalui internet, *political hacking, cyberterrorism, cyberbullying* dan sebagainya.[23]

Kejahatan yang berhubungan dengan komputer merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan peralatan komputer.[24] Dari pemahaman tersebut, *Cyber crime* dapat dibagi menjadi dua kategori, dalam pengertian sempit dan dalam pengertian luas. *Cyber crime* dalam pengertian sempit merupakan kejahatan terhadap sistem komputer, sedangkan *cyber crime* dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer.[25]

4. Peran Intelijen Keamanan Dalam Pencegahan Tindak Pidana *Cyber Crime*

Tindak pidana yang terjadi di berbagai daerah di Indonesia tidak terlepas dari berbagai masalah hukum, sosial, ekonomi, politik dan sebagainya dalam masyarakat Untuk dapat mengantisipasi dan mencegah terjadinya tindak pidana, baik yang dilakukan secara perorangan maupun kelompok massa, Intelkam Polri mempunyai peranan yang sangat penting dalam institusi Kepolisian Republik Indonesia. Peran fungsi Intelkam sebagai basis deteksi dini dari berbagai kegiatan operasional kepolisian, sebagai mata dan telinga (indera) bagi pimpinan pada semua level organisasi dari tingkat Mabes Polri sampai Polsek sebagai lini terdepan.

Peran Intelkam sebagai pelaksana fungsi Intelkam keamanan yang meliputi penyelidikan, pengamanan dan penggalangan dalam rangka terciptanya stabilitas

[22] Dian Ekawati Ismail, 2009, *Cyber Crime di Indonesia*, Jurnal Inovasi, Vol. 6 No. 3, hlm. 243
[23] Dewi Bunga, *Loc.cit*
[24] Sri Sumarwani, Op.cit, hlm. 288
[25] Muhammad Anthony Aldriano dan Mas Agus Priyambodo, 2022, *Cybercrime Dalam Sudut Pandang Hukum Pidana*, Jurnal Kewarganegaraan, Vol. 6 No. 1, hlm. 2169

keamanan dan ketertiban masyarakat. Oleh karena itu keberadaan intelkam harus dapat mengantisipasi berbagai perkembangan situasi sehingga apabila muncul ancaman faktual dapat ditangani secara profesional dan proporsional sesuai dengan prosedur yang ditetapkan dalam peraturan perundang-undangan. Dalam Teori Peran tersirat bahwa peran intelkam Polri dapat menjadi personal yang merupakan penghubung dan penjaga dinamika sosial yang berkembang dalam masyarakat terkhusus dalam konsep masyrakat yang tergabung dalam sebuah organisasi. Peran ini sangat vital dalam hal menjaga agar tidak terjadi konflik sosial.

Terkait dengan tindak pidana *cyber crime*, dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, terdapat kelompok kejahatan digital, yakni *Computer Related Company* diantaranya Penipuan, Ujaran Kebencian, Pengancaman dan *Computer Crime* diantaranya Peretasan Sistem Elektronik, *Ilegal Interseption*, Perubahan tampilan *Website*. Adapun materi yang disampaikan tentang tindak pidana yang ditangani dalam UU ITE yakni Pencemaran nama baik / penghinaan, ujaran Kebencian dengan unsur SARA, menyebarkan berita bohong / Hoax, ilegal akses, pencurian data, *hacking*, penipuan online dan judi online.

Peran yang dilaksanakan oleh Intelkam Polri dalam mencegah terjadinya tindak pidana *Cyber Crime* adalah peran normatif dan faktual. Peran normatif dilaksanakan berdasarkan ketentuan dalam peraturan perundang-undangan. Dalam Pasal 13 Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia yang menyebutkan bahwaTugas pokok Kepolisian Negara Republik Indonesia adalah:

a. memelihara keamanan dan ketertiban masyarakat;
b. menegakkan hukum; dan
c. memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat.

Dasar hukum lain peran intelkam Polri adalah Pasal 40 ayat (2) Undang-Undang Nomor 19 Tahun 2016 yang menyatakan :

Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan peraturan perundang-undangan.

(2a) Pemerintah wajib melakukan pencegahan penyebarluasan dan penggunaan Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan.

(2b) Dalam melakukan pencegahan sebagaimana dimaksud pada ayat (2a), Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan pemutusan akses

terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar hukum.

Dalam hal ini Polri dalam mencegah Kejahatan Dunia Maya dengan Kegiatan Operasional yakni Preemtif dan Preventif sebagai bentuk Sosialisasi, Patroli Siber, dan Edukasi Siber. Tindakan preemtif merupakan upaya awal yang dilakukan untuk mencegah terjadinya tindak pidana *cyber crime* dengan menanamkan nilai-nilai atau norma-norma, sehingga dapat terealisasi dalam diri seseorang. Cara ini mengupayakan menghilangkan niat seseorang untuk melakukan kejahatan *cyber crime* meskipun ada kesempatan untuk melakukannya. Tindakan preventif merupakan segala usaha, pekerjaan, kegiatan, ataupun usaha penecegahan yang memaksa lawan meninggalkan bekas bila berhasil menerobos serta mencegah hambatan-hambatan yang bersumber dari pihak sendiri maupun pihak yang mengakibatkan suatu bencana.[26] Tindakan preventif terhadap *cyber crime* merupakan tindakan yang mengharapkan kejahatan tersebut dapat ditanggulangi dan dicegah sebelum kejahatan itu terjadi dalam hal yang lain mengharapkan terjadinya penurunan dari kejahatan tersebut atau kejahatan tersebut dapat dihilangkan.[27]

Patroli siber merupakan patroli yang dilakukan di dalam kepolisian dalam pelaksanaannya patroli siber yang bertujuaan untuk mengawasi segala macam bentuk pelanggaran terhadap hukum di dalam internet terkhusus aplikasi media sosial. Patroli siber dapat dilakukan pada aplikasi media sosial, seperti instagram, whatsapp, *twitter*, dan sebagainya. Patroli siber dilakukan untuk menciptakan ruang internet yang aman serta melindungi masyarakat dari kejahatan.[28] Edukasi Siber merupakan sebuah pengenalaan akan *cyber crime* dan bahayanya. Edukasi siber lebih lagi ditujukan untuk memberikan manfaat informasi tentang *cyber crime* keseluruhan baik, bahayanya, jenis-jenisnya, modusnya serta hukuman akan kejahatan tersebut.

Sementara itu, peran faktual dilaksanakan oleh Intelkam Kepolisian dalam penanggulangan tindak pidana *cyber crime* dengan berdasar pada fakta ancaman yang terjadi dalam kehidupan masyarakat. Jika terdapat informasi Intelkam Kepolisian mengenai situasi ancaman terjadinya tindak pidana cyber crime, maka pihak Kepolisian dapat melakukan *Take Down*. Take down merupakan salah satu strategi dari lima bentuk pencegahan yang dilakukan oleh Polri dalam mencegah cyber crime. *Take down* merupakan suatu tindakan untuk menghentikan ataupun menghapus ketersediaan sesuatu yang berada dalam ruang internet seperti video, website, berita ataupun aplikasi yang kurang baik, seperti melanggar etika, moral dan kesopanan serta hukum.[29]

[26] Y. Wahyu Saronto, *Op.cit*, hlm. 60.
[27] Andreas Agung dan Hafrida, Erwin, 2022, *Pencegahan Kejahatan Terhadap Cybercrime*, Pampas: Journal of Criminal, Vol.3 No. 2, hlm. 218
[28] Ibid, hlm. 219
[29] Ibid, hlm. 220

Dalam konteks pencegahan tindak pidana *cyber crime* oleh Intelkam Polri, dibutuhkan manajemen resiko. Adapun tahapan dalam manajemen resiko yang dilakukan adalah : [30]

a. Identifikasi

Pada tahap ini, identifikasi risiko *cyber crime* dilakukan secara berkala terhadap pemicu terjadinya kejahatan tersebut. Dalam proses ini, seluruh aspek yang berpotensi menimbulkan kerugian diidentifikasi dengan seksama. Seluruh risiko yang teridentifikasi selanjutnya diukur. Ukuran risiko pada ancaman ini mengacu pada dua ukuran, yaitu Probabilitas dan Dampak Probabilitas.

b. Penilaian

Pada tahap ini, dilakukan penilaian terhadap tingkat risiko yang ditimbulkan dari *cyber crime* yang berdampak pada seluruh aspek kehidupan terutama pada keamanan dan pertahanan negara. Penilaian terhadap *cyber crime* tidak dapat diukur secara langsung namun bisa menggunakan tabel matriks dalam pengukuran risiko yang ditimbulkan akibat *cyber crime.*

c. Perlakuan

Setelah melakukan identifikasi dan pengukuran risiko, selanjutnya digunakan sebagai dasar untuk menentukan perlakuan dan respons terhadap risiko, apakah risiko akan diterima, dialihkan, diminimalisir atau dihindari. Dalam kasus ini, perlu dilakukan minimalisir terhadap penyalahgunaan atau pencurian informasi dan data yang sering terjadi baik secara individu maupun lembaga.

d. Kontrol dan Pemantauan

Pemantauan dan penyesuaian terus dilakukan untuk menilai keberhasilan manajemen risiko. Dalam proses pemantauan, terdapat mekanisme peringatan dini bagi pihak pengendali keamanan, sehingga pihak pengendali dapat melakukan tindakan-tindakan yang dianggap perlu agar bisa mengantisipasi adanya *cyber crime*.

Dalam memberikan gambaran tentang tindak pidana *cyber crime* yang akan dihadapi, intelkam mempunyai Intelijen yang diramalkan (*Forecasting*) yang mempunyai peranan penting bagi intelijen, karena dapat meramalkan perkembangan situasi yang akan terjadi di masa datang sebagai lanjutan proses perkembangan yang sedang terjadi. Setiap informasi yang diberikan anggota intelkam Polri yang bertujuan memberikan masukan kepada pimpinan untuk melakukan deteksi dini tidak semata-mata diberikan secara mentah, tetapi melalui tahapan-tahapan pengolahan dengan analisa yang tinggi. Dengan demikian intelijen yang diramalkan mempunyai arti sebagai *early warning* bagi pihak yang bertanggung jawab untuk menentukan rencana dan langkah-langkah dalam mencegah terjadinya tindak pidana *cyber crime*.

[30] Ineu Rahmawati Op.cit, , hlm. 58

5. Kendala yang Dihadapi Intelijen Kepolisian Dalam Menanggulangi Tindak Pidana *Cyber Crime*

Cyber Crime merupakan tindak pidana yang dilakukan dengan memanfaatkan kemajuan teknologi informasi dan komunikasi. Perkembangan dunia kejahatan yang menggunakan teknologi informasi dan komunikasi tentu saja perlu diimbangi dengan perkembangan metode dan pola kerja Kepolisian dalam menangani kejahatan tersebut. Artinya bahwa Kepolisian juga dituntut untuk dapat mengikuti perkembangan situasi masyarakat yang dalam hal ini bentuk kejahatan dengan memperkuat serta melengkapi diri menghadapi ancaman tindak pidana *Cyber Crime*. Dalam mencegah terjadinya tindak pidana *cyber crime*, maka intelkam memiliki peran yang sangat besar dalam melakukan penyelidikan dan juga deteksi dini.

Pada tingkat Kepolisian Daerah (Polda) Sulawesi Selatan, jumlah kasus tindak pidana *cyber crime* sejak Januari tahun 2023 hingga Juni 2023 mencapai 172 kasus. Pada wilayah Kepolisian Resor Kota Besar (Polrestabes) Makassar, jumlah tindak pidana *cyber crime* terbilang cukup besar. Pada tahun 2022 jumlah kasus tindak pidana *cyber crime* adalah sebanyak 383 kasus. Pada Januari hingga Juni tahun 2023, jumlah tindak pidana *cyber crime* adalah sebanyak 71 kasus. Dari jumlah kasus tersebut, mayoritas tindak pidana *cyber crime* yang dilakukan berupa ujaran kebencian *(hate speech)*, teror melalui media sosial, pencemaran nama baik, dan kampanye hitam mengingat adanya situasi menjelang Pemilihan Umum.

Kepala Urusan Bin Operasional (KBO) Satuan Intelijen Keamanan Polrestabes Makassar, Inspektur Polisi Satu Suhartoyo, upaya-upaya yang telah dilakukan oleh personel intelkam untuk mencegah terjadinya tindak pidana *cyber crime* adalah melakukan pendekatan personal kepada kelompok-kelompok anak muda, khususnya kelompok pakar dan pemerhati Informasi Teknologi, penyuluhan hukum mengenai undang-undang ITE serta tindak pidana *cyber crime,* dan memaksimalkan bantuan serta keterlibatan masyarakat sipil. Secara teknis, intelkam juga sering melakukan peretasan dan *take down* akun media sosial yang diduga mengandung unsur tindak pidana *cyber crime*. Dalam hal kegiatan intelijen, intelkam juga melakukan upaya penggalangan terhadap kelompok-kelompok masyarakat ahli dalam bidang informasi teknologi dengan maksud agar mempermudah kerja intelkam dalam mencegah terjadinya tindak pidana *cyber crime*.

Namun dalam perjalanannya, upaya yang dilakukan oleh Intelkam untuk mencegah terjadinya tindak pidana *cyber crime* dapat dikatakan belum cukup optimal. Kemampuan panca indera yang dimiliki oleh personel intelkam sangat terbatas dalam melihat, mengamati, menggambarkan, merekam suatu data, fakta dan informasi. Dalam hal ini, terdapat berbagai kendala baik kendala, yang bersifat internal maupun eksternal. Adapun kendala internal yang dihadapi oleh pihak kepolisian adalah terkait dengan sumber daya manusia dan juga sarana prasarana.

Pengelolaan Sumber Daya Manusia dalam institusi kepolisian, khsusunya Intelijen keamanan menjadi hal yang sangat penting sebagai salah satu kunci keberhasilan dalam upaya pencegahan dan penanganan tindak pidana *Cyber Crime*. Dalam hal pengembangan sumber daya manusia, terdapat dua hal yang perlu diperhatikan, yaitu dari segi kuantitas dan kualitas personel kepolisian. Berkaitan dengan kuantitas, rasio jumlah personel Polri secara keseluruhan saat ini adalah 1:1.300, yang berarti bahwa seorang anggota Polri harus mengawasi dan memantau kegiatan 1.300 orang masyarakat. Hal ini jelas merupakan kondisi yang mustahil bisa dilaksanakan dengan baik.[31]

Tugas polri dalam menjaga kamtibmas dilakukan dengan mengedepankan Kepolisian Sektor (Polsek) sebagai ujung tombak, karena langsung berhubungan dengan masyarakat. Ketika terjadi permasalahan kamtibmas, maka Polsek yang pertama kali menghadapi permasalahan tersebut. Terkait dengan tugas intelkam, peran Polsek adalah sebagai basis deteksi yang juga merupakan peran ganda Polsek dalam pelaksanaan fungsi Polsek sebagai ujung tombak kepolisian. Hanya saja, tugas-tugas tersebut terbatas, karena minimnya jumlah personel dalam setiap Polsek. Secara umum, jumlah personel masih minim, sehingga Polsek hanya mampu melakukan kegiatan penjagaan markas, pelayanan masyarakat seperti menerima laporan dan pengaduan masyarakat. Untuk pelaksanaan fungsi lain hanya berupa kegiatan awal saja, sehingga membutuhkan dukungan dari Kepolisian Resor, seperti penyidikan, pembinaan masyarakat, intelijen, dan kegiatan preventif lainnya.[32]

Pada wilayah Polrestabes Makassar, jumlah personel Kepolisian juga masih terbatas. Berdasarkan hasil wawancara dengan Kepala Urusan Bin Operasional (KBO) Satuan Intelijen Keamanan Polrestabes Makassar, Inspektur Polisi Satu Suhartoyo, secara ideal rasio jumlah personel kepolisian adalah 1 : 100 atau 1 : 200, di mana satu anggota Kepolisian menjaga dan mengawasi 100 atau 200 orang masyarakat. Akan tetapi, untuk wilayah Kota Makassar, perbandingan julah personel Kepolisian adalah 1 : 1.000. Menurutnya, jumlah tersebut tidak memadai untuk melaksanakan tugas kepolisian secara makasimal. Terkait unit intelijen, jumlah ideal personel intelijen keamanan di tiap Polsek adalah sebanyak 13 sampai 14 orang.

Pada jajaran Polrestabes Makassar, jumlah personel Satuan Intelkam sebanyak 98 orang, yang terdiri dari 2 orang berpangkat Perwira Menengah (Pamen), 18 berpangkat Perwira Pertama (Pama), 76 berpangkat Bintara, dan 2 orang Pegawai Negeri Sipil. Berikut daftar jumlah personel intelkam di tiap Polsek wilayah Kota Makassar. Berdasarkan data yang diperoleh, jumlah personel intelkam di setiap Polsek di wilayah Kota Makassar tidak mencapai jumlah ideal menurut Perkapolri. Dalam hal pencegahan tindak pidana *cyber crime*, dengan jumlah personel tersebut

[31] Y. Wahyu Saronto, Op.cit, hlm. 11
[32] Ibid, hlm. 103

tentu sangat terbatas. Menurut Inspektur Polisi Satu Suhartoyo, dugaan tindak pidana *cyber crime* harus dilaporkan ke tingkat Polrestabes hingga Polda. Namun dengan kondisi terbatasnya jumlah personel, maka pelaporan mengenai dugaan tindak pidana *Cyber Crime* tersebut menjadi terlambat. Akibatnya, keputusan untuk melakukan eksekusi atau tindakan yang akan diambil untuk dugaan tersebut juga menjadi terlambat. Dengan keterbatasan jumlah personel tersebut, untuk proses penyelidikan dari laporan hingga ke tahap sidik membutuhkan waktu selama 14 hari hingga 20 hari.

Selain kendala dalam hal keterbatasan jumlah personel, kendala lain yang terkait dengan ketersediaan sumber daya manusia adalah dalam hal kemampuan atau kualitas personel. Keterbatasan ini pada dasarnya hampir dialami jajaran kepolisan di Indonesia. Secara umum, kemampuan personel intelkam dalam pengunaan komputer dan pemahaman terhadap *cyber crime, hacking*, dan bentuk-bentuk *cyber crime* lainnya masih minim. Selain itu, pengalaman terkait penanganan kasus *cyber crime* pun dapat dikatakan masih cukup minim.[33]

Pada jajaran Polrestabes Makassar, dapat dikatakan bahwa jumlah personel Intelkam yang telah mengikuti pelatihan yang terkait dengan bidang intelkam atau pendidikan kejuruan masih sangat minim. Berbagai penyebab menjadi alasan dari kondisi ini, diantaranya faktor usia, anggaran, dan juga keluarga. Berdasarkan data yang dimiliki pada bulan Maret tahun 2022, dari 93 personel Intelkam Polrestabes Makassar, hanya sebanyak 37 personel yang telah mengikuti atau mendapat pendidikan kejuruan dengan berbagai macam bidang terkait bidang intelkam.

Faktor lain yang memiliki peran sentral dalam pelaksanaan tugas dan fungsi intelkam adalah sarana dan prasana, yang dalam hal ini terkait dengan anggaran dan peralatan. Terkait alat-alat yang digunakan dalam pelaksanaan tugas intelkam, telah diatur dalam Surat Keputusan Kapolri Nomor : Skep / 991 / XII / 2005 tanggal 30 Desember 2005, tentang Sistem Pembinaan Alat Khusus Intelijen. Alat Khusus Intelijen didefinisikan sebagai semua bentuk peralatan, baik yang bersifat statis maupun dinamis, yang berfungsi sebagai alat bantu untuk mendukung tugas/kegiatan Intelijen. Berdasarkan Surat Keputusan Kapolri Nomor 992/2005 tentang Standarisasi Alsus Intel, telah menentukan jenis peralatan yang harus dimiliki oleh setiap satuan intelijen, baik ditingkat Mabes, Polda, Polres/Ta dan Polsek.

Penggolongan alat khusus (Alsus) intelijen Polri terdiri dari Alsus Deteksi, Alsus Pengamanan, dan Alsus Komunikasi. Berdasarkan kegunaannya, Alsus intel dikelompokkan menjadi 13 kegunaan, yaitu untuk observasi, merekam suara, merekam gambar bergerak (video) dan tidak bergerak (photo), menyadap suara, menyadap video, komunikasi, pengamanan, deteksi barang-barang berbahaya,

[33] Dista Amalia Arifah, 2011, *Kasus Cybercrime di Indonesia*, Jurnal Bisnis dan Ekonomi (JBE), , Vol. 18, No. 2, hlm 192

membuka pintu dan tas kopor, transportasi, pengolah data, mengacau alat penyadap lawan, melacak alat penyadap lawan.[34] Peralatan khusus intelijen tersebut berfungsi sebagai alat bantu dalam mendukung tugas serta kegiatan intelijen yang terdiri dari berbagai jenis, spesifikasi teknis dan desain peralatan, baik yang sifatnya statis maupun dinamis.

Beberapa jenis peralatan ideal yang dibutuhkan dalam pelaksanaan tugas intelkam adalah alsus observasi berupa *night google vision (teropong malam)*, *surveillance binocular (teropong)*, *photosnipper surveillance*, *handycame* dan *camera digital, HT, mobile repeater, portable repeater, body vest, lock picking set* dan *active interceptor*, pengacak signal *handphone*, alat sadap, *digital camera* dengan lensa tele untuk pengambilan gambar jarak jauh, dan beberapa jenis *spy cam* dalam berbagai bentuk.[35] Berdasarkan penelitian yang dilakukan oleh S. Sumarjiyo, jika dilihat dari segi kuantitas dan kualitas, peralatan khusus intelijen masih belum memadai jika dibandingkan dengan kondisi ideal yang diharapkan. Teknologi yang digunakan pada alsus intelkam masih bervariasi, yaitu menggunakan teknologi lama dan teknologi baru. Keterbatasan ini salah satunya disebabkan oleh keterbatasan dana untuk pengadaan peralatan khusus intelijen. Kondisi peralatan yang terbatas secara otomatis berdampak pada kinerja personil intelkam yang juga terbatas.

Salah satu tugas utama dari intelkam adalah melakukan deteksi dini terhadap situasi kamtibmas. Oleh karena itu, peralatan intelkam yang sangat diperlukan adalah alat khusus deteksi dini. Namun, alat deteksi tersebut sebagian besar belum dimiliki, khususnya di tingkat Polsek. Personel intelkam pada umumnya menggunakan handphone pribadi untuk melakukan komunikasi sekaligus sebagai alat untuk merekam suara dan gambar. Belum lagi soal kualitas alat yang dimiliki yang juga masih terbatas, sehingga belum berfungsi secara optimal.

Menurut Inspektur Polisi Satu Suhartoyo di wilayah Polrestabes Makassar, sarana alat khusus intelijen masih sangat terbatas. Di tingkat Polsek, unit intelkam tidak dilengkapi dengan alat deteksi khusus, sehingga personel masih menggunakan peralatan pribadi seperti handphone. Untuk melakukan *take down* atau peratasan akun media sosial yang diduga melakukan tindak pidana *cyber crime* hanya dapat dilakukan di tingkat Polrestabes dan Polda. Anggaran yang tersedia untuk melengkapi peralatan intelkam juga masih sangat minim. Pada tahun 2023, setiap bulan rata-rata anggaran yang disiapkan untuk dana deteksi hanya sebesar Rp2 juta. Jumlah ini tentu saja sangat minim jika dibandingkan dengan tugas deteksi dini yang harus dilakukan unit intelkam.

Untuk Satuan Intelkam Polrestabes Makassar sendiri pada dasarnya terdapat upaya untuk meningkatkan kuantitas dan kualitas sarana dan prasarana intelkam.

[34] S. Sumarjiyo, 2018, *Efektivitas Peralatan Intelijen Polri Dalam Rangka Deteksi Dini Guna Mencegah Tindak Pidana*, Jurnal Litbang Polri, Vol. 21, No. 1, hlm. 150
[35] Ibid, hlm. 167

Setiap tahun dapat dikatakan terdapat peningkatan anggaran sebesar 20 persen untuk pelaksanaan tugas dan fungsi intelkam. Namun, hal tersebut juga masih terbatas untuk mengadakan peralatan intelkam yang ideal. Salah satu alat khusus intelkam yang terkait dengan tindak pidana *cyber crime* yang canggih adalah alat dinamis yaitu kendaraan taktikal yang disebut *tactical telecommunication monitoring system* yang dimiliki Polda Sulawesi Selatan sebanyak 2 unit. Alat deteksi ini dapat digunakan untuk penyadapan, memutus signal, broadcast *Short Message Service (SMS)* dan *Whatsapp* untuk semua *provider*.

Pada tingkat Polda Sulawesi Selatan, peralatan intelkam yang telah dimiliki adalah *night google vision (teropong malam)*, *surveillance binocular (teropong)*, *photosnipper surveillance*, *handycame* dan *camera digital, HT, mobile repeater, portable repeater, body vest, lock picking set* dan *active interceptor,* pengacak signal *handphone*, alat sadap, *digital camera* dengan lensa tele untuk pengambilan gambar jarak jauh, dan beberapa jenis *spy cam* dalam berbagai bentuk. Sedangkan pada tingkat Polrestabes Makassar, peralatan yang tersedia yaitu *handycame* dan *camera digital, HT, mobile repeater, portable repeater, body vest, lock picking set* dan *active interceptor,* pengacak signal *handphone*, alat sadap, *digital camera* dan *spy cam*. Secara umum, peralatan deteksi yang dimiliki pada dasarnya masih menggunakan teknologi yang sederhana dan belum mampu merekam suatu aktivitas secara mendetail dan tingkat akurasi yang tinggi. Dari sudut pandang desain, peralatan yang ada belum memiliki desain yang sesuai dengan karakteristik kegiatan intelijen di lapangan yang dilakukan secara sembunyi atau rahasia.

Keterbatasan peralatan lain adalah keberadaan komputer forensik untuk melacak jejak para pelaku tidak pidana *cyber crime*, terutama yang berhubungan dengan program-program data komputer. Sarana ini diperlukan untuk dapat mengungkap data digital serta merekam dan menyimpan bukti berupa *soft copy* (*image*, program, dan sebagainya) yang bisa melayani tiga hal penting yaitu *evidence collection*, *forensic analysis*, *expert witness*. Jika dibandingkan dengan negara yang telah memiliki satuan intelkam yang kuat, maka keberadaan sarana dan prasarana intelkam masih jauh tertinggal.

6. Kesimpulan

Peran intelkam dalam mencegah terjadinya tindak pidana Cyber Crime terdiri dari peran normatif dan peran faktual. Peran normatif dilaksanakan berdasarkan ketentuan dalam peraturan perundang-undangan, dimana dalam hal ini intelkam berperan sesuai dengan peraturan perundang-undangan yang terkait dengan tindak pidana *Cyber Crime*. Berdasarkan peraturan perundang-undangan tersebut, Intelkam mencegah tindak pidana *Cyber Crime* dengan kegiatan operasional yakni Preemtif dan Preventif sebagai bentuk Sosialisasi, Patroli Siber, dan Edukasi Siber. Sedangkan peran faktual dilaksanakan oleh Intelkam Kepolisian dalam penanggulangan tindak

pidana *cyber crime* dengan berdasar pada fakta ancaman yang terjadi dalam kehidupan masyarakat. Jika terdapat informasi mengenai situasi ancaman terjadinya tindak pidana *cyber crime*, maka pihak Kepolisian dapat melakukan *Take Down*.

Kendala-kendala yang dihadapi oleh Intelkam dalam mencegah tindak pidana *cyber crime* merupakan kendala yang berasal dari internal kepolisian, yaitu faktor sumber daya manusia dan sarana prasarana. Dalam hal ini, kendala dalam hal sumber daya manusia adalah minimnya jumlah personel intelkam, khususnya yang berada di tingkat Polsek sebagai ujung tombak dalam tugas intelkam. Selain dalam hal kuantitas, kendala lain terkait sumber daya manusia adalah dari segi kualitas, yaitu tingkat pengetahuan personel intelkam masih belum memadai. Dalam hal ini, masih sangat sedikit personel intelkam yang telah memperoleh pedidikan kejuruan yang terkait dengan intelijen, khususnya mengenai *cyber crime*. Hal ini disebabka karena beberapa hal, seperti usia, anggaran dan juga keluarga. Kendala dalam hal sarana prasarana terkait dengan keterbatasan jumlah peralatan intelejen, khsusunya yang terkait dengan *cyber crime*. Keterbatasan peralatan ini paling dirasakan di tingkat Polsek. Selain dalam hal kuantitas peralatan, kendala lain adalah kualitas peralatan yang tersedia, di mana teknologi yang digunakan masih tergolong teknologi sederhana.

Referensi

Abdul *Wahid* dan Mohammad *Labib*, 2010, *Kejahatan Mayantara*. Refika Aditama, Bandung.

Abdussalam, H. R. 2009. *Hukum Kepolisian Sebagai Hukum Positif dalam Disiplin Hukum.* Restu Agung, Jakarta.

Achmad Ali, 2011, *Menguak Tabir Hukum*. Ghalia Indonesia, Bogor.

Adam Chazawi, 2003, *Kejahatan Terhadap Harta Benda*, Bayu Media, Malang.

_____, 2011, *Pelajaran Hukum Pidana Bagian I,* Rajawali Pers, Jakarta.

Andreas Agung dan Hafrida, Erwin, 2022, *Pencegahan Kejahatan Terhadap Cybercrime*, Pampas: Journal of Criminal, Vol.3 No. 2

Ary Purwanti, Burham Pranawa, Purwadi, 2021, *Deteksi Dini Oleh Intelkam Polri Dalam Mengantisipasi Gangguan Kamtibmas Pada Pilkada di Boyolali*, Jurnal Bedah Hukum, Vol. 5 No.1.

Bisri Ilham, 1998, *Sistem Hukum Indonesia*, Grafindo Persada, Jakarta.

Budi Suhariyanto, 2012 *Tindak Pidana Teknologi Informasi (Cybercrime)-Urgensi Pengaturan dan Celah Hukumnya,* Rajawali Pers, Jakarta.

Dewi Bunga, 2019, *Politik Hukum Pidana Terhadap Penanggulangan Cyber Crime*, Jurnal Legislasi Indonesia, Vol. 16 No. 1.

Dian Ekawati Ismail, 2009, *Cyber Crime di Indonesia*, Jurnal Inovasi, Vol. 6 No. 3.

Didik M. Arief Mansur dan Elisatris Gultom, 2005**,** *Cyber Law: Aspek Hukum Teknologi Informasi,* Refka Aditama, Bandung.

H. Pudi Rahardi, 2007, *Hukum Kepolisian (Profesionalisme dan Reformasi Polri)*, Penerbit Laksbang Mediatama, Surabaya.

H. Sutarman, 2007, *Cyber Crime-Modus Operandi dan Penanggulangannya*, Laksbang Pressindo, Yogyakarta.

Ineu Rahmawati, 2017, *Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defence*, Jurnal Pertahanan dan Bela Negara, Vol. 7 No. 2.

Ketut Adi Purnama, 2018, *Hukum Kepolisian Sejarah dan Peran POLRI Dalam Penegakan Hukum serta Perlindungan HAM,* Refika Aditama, Bandung.

Lita Sari Malita, 2015, *Cyber Crime dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law di Indonesia*, Jurnal Cakrawala Vol. 15 No. 2.

M. Ali Zaidan, 2015, *Menuju Pembaruan Hukum Pidana,* Sinar Grafika, Jakarta.

Mahrus Ali, 2011, *Dasar Dasar Hukum Pidana*, Ctk. Pertama, Sinar Grafika, Jakarta.

Marlina. 2011, *Hukum Penitensier*, Refika Aditama, Bandung.

Maurice Duverger, 2010, *Sosiologi Politik*, Rajawali Pers, Jakarta

Moeljatno, 1993, *Asas-Asas Hukum Pidana*, Rineka Cipta, Jakarta.

Muhammad Anthony Aldriano, Mas Agus Priyambodo, 2022, *Cyber Crime Dalam Sudut Pandang Hukum Pidana*, Jurnal Kewarganegaraan Vol. 6 No. 1.

Momo Kelana, 1984, *Hukum Kepolisian,* Edisi ketiga, PTIK, Jakarta.

Morissan, 2005. *Hukum Tata Negara RI Era Reformasi,* Ramdina Prakarsa, Jakarta.

Muladi Dan Barda Nawawi Arief, 2010, *Teori-Teori Dan Kebijakan Pidana*, Alumni, Bandung.

Mulyati Pawennei dan Rahmanuddin Tomalili, 2015, *Hukum Pidana*, Mitra Wacana Media, Jakarta.

P.A.F. Lamintang, 1984, *Dasar-Dasar Hukum Pidana Indonesia,* Sinar Baru, Bandung.

Priyo Widyanto, 2016, *Tugas Pokok dan Fungsi Intelkam,* Mediacom, Balikpapan.

Ramadhan, N. A, 2018, *Peran Intelkam Polda Lampung Dalam Mengidentifikasi Ancaman Terhadap Gangguan Kamtibmas.* Fakultas Hukum Universitas Bandar Lampung.

Sadjijono, 2006, *Hukum Kepolisian, Perspektif Kedudukan dan Hubungan Dalam Hukum Administratif*, Laksbang PRESSindo, Yogyakarta.

Sri Sumarwani, 2014, *Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif*, Jurnal Pembaharuan Hukum, Vol. 1 No. 3.

Stainislaus Riyanta, 2015, *Kajian Stratejik Intelijen,* Universitas Indonesia: Jurnal Intelijen, Jakarta.

Tim Penyusun, 2012, *Naskah Pencerahan Intelkam*, Baintelkam Polri, Jakarta.

Y. Sumarjiyo, 2018, *Efektivitas Peralatan Intelijen Polri Dalam Rangka Deteksi Dini Guna Mencegah Tindak Pidana*, Jurnal Litbang Polri, Vol. 21, No. 1.

Yosua Praditya Suratman, 2017, *Penggunaan Strategi Operasi Kontra Intelijen Dalam Rangka Mengahadapi Ancaman Siber Nasiona*l, Jurnal Pertahanan dan Bela Negara, Vol. 7 No. 2.

Polri: Indonesia Tertinggi Kedua Kejahatan Siber di Dunia, dalam website https://www.kominfo.go.id/content/detail/13487/polri-indonesia-terfinggi-kedua-kejahatan-siber-di-dunia/0/sorotan_media, diakses tanggal 2 Maret 2023

Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2017 tentang Susunan Organisasi dan Tata Kerja Satuan Organisasi Pada Tingkat Markas Besar Kepolisian Negara Republik Indonesia.

Peraturan Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2018 tentang Susunan Organisasi dan Tata Kerja Kepolisian Daerah.

Peraturan Kepolisian Negara Republik Indonesia Nomor 2 Tahun 2021 tentang Susunan Organisasi dan Tata Kerja Pada Tingkat Kepolisian Resor dan Kepolisian Sektor

Peraturan Kepala Badan Intelijen Keamanan Kepolisian Negara Republik Indonesia Nomor 4 Tahun 2012 tentang Pertelaan Tugas di Lingkungan Badan Intelijen Keamanan Kepolisian Negara Republik Indonesia