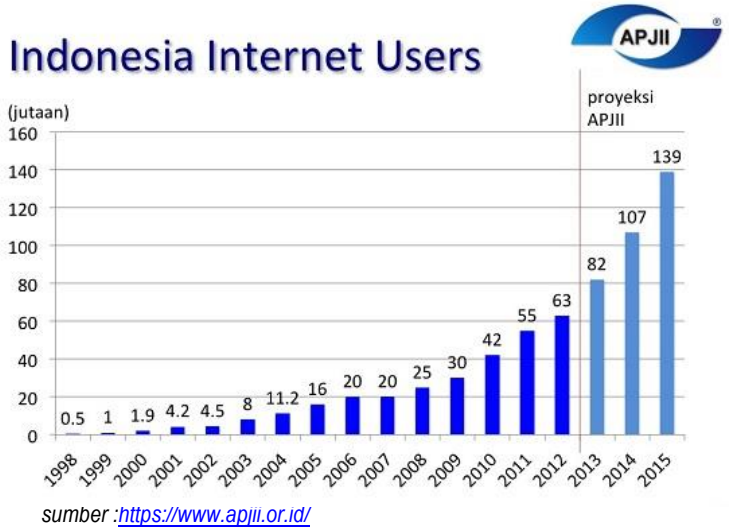
BAB I
PENDAHULUAN

A. Latar Belakang

Era virtual yang berakibat pada terciptanya suatu fenomena positif yang membuat interaksi publik apakah antara individu maupun kelompok menjadi lebih mudah. Situasi baru ini sebagai akibat dari revolusi teknologi informasi dan berkembangnya teknologi yang semakin pesat bahkan situasi terakhir sudah pada tahapan nirkabel. Pertumbuhan pengguna teknologi informasi dalam hal ini pengguna internet menjadi sangat signifikan dan bahkan trend yang terjadi sudah menjadi suatu keniscayaan. Artinya individu maupun kelompok yang tidak mampu beradaptasi dengan era virtual ini maka kemampuan bertahan hidupnya atau kemampuan mengembangkan dirinya akan mengalami degradasi. Kita dapat melihat situasi terkini bahkan akan aneh seorang individu tanpa memiliki alat komunikasi. Asosiasi Penyelenggara Jasa Internet Indonesia bahwa pengguna internet telah berkembang sangat signifikan di tanah air.



sumber :https://www.apjii.or.id/

Gambar 1. Indonesia Internet users

Perkembangan teknologi yang meniscayakan masyarakat untuk berinteraksi dengan menggunakannya demikian juga dengan para pelaku kejahatan. Masyarakat Indonesia yang terdiri dari 255 juta penduduk, terdapat

139 juta pengguna internet, 88 juta diantaranya pengguna internet aktif, dan 326 juta pengguna peralatan telekomunikasi mobil *(mobile phone)*, dimana 79 juta diantaranya aktif menggunakan media sosial, hal ini tentunya menjadi suatu tantangan bagi penegak hukum untuk melakukan antisipasi terhadap akibat negatif berupa perbuatan melawan hukum yang harus diungkap, terutama dalam memperoleh informasi/ alat bukti yang tersimpan pada peralatan elektronik yang dikuasai saksi/ tersangka, maupun yang tersimpan pada *server-server* penyedia layanan internet.

sumber :http://wearesocial.com/

Gambar 2. Pengguna Internet di Indonesia

Polri telah melakukan antisipasi sejak empat belas tahun yang lalu, dan akhirnya pada Tahun 2002 dengan membentuk Subdit IT & *Cyber Crime* berdasarkan Surat Keputusan Kapolri Nomor 53 dan 54 tahun 2002, yang saat itu bernama Unit *Cyber* Crime, dipimpin seorang Pamen berpangkat Komisaris Polisi, dan berada dibawah Direktorat Tindak Pidana Ekonomi dan Khusus Bareskrim Polri. Nomenklatur ini kemudian dirubah berdasarkan Perkap Nomor 21 Tahun 2010 tentang Susunan Organisasi Dan Tata Kerja pada tingkat Markas Besar Kepolisian Negara Republik Indonesia dan Perkap Nomor 22 Tahun 2010 tentang Susunan Organisasi Dan Tata Kerja Pada Tingkat Kepolisian Daerah, menjadi Subdirektorat IT dan *Cyber Crime* Dit Tipideksus Bareskrim Polri. Pada tahun 2011 Kepolisian Negara Republik Indonesia mendapat hibah dari *Australian Federal Police* berupa fasilitas *Cyber Crime*

Investigation Center. Saat ini seluruh hibah dari Australian Federal Police sudah masuk ke dalam Sistem Informasi Manajemen dan Akuntansi Barang Milik Negara (SIMAK BMN), hibah tersebut meliputi fasilitas Penyelidikan dan Penyidikan *Cybercrime*, dan fasilitas Unit Digital Forensik yang dilengkapi Almatsus seperti *Accessdata Forensik Toolkit*, *Encase, Xways, Cellebrite, XRY,* dll. Namun demikian bahwa tantangan yang menjadi tanggung jawab Polri terkait virtualisasi, diperlukan suatu evaluasi untuk menjawab kebutuhan publik dalam rangka mewujudkan kehadiran negara ditengah masyarakat abad ini.

Pada tahun 2015 sebanyak 2.522 tindak pidana siber dilaporkan baik dalam bentuk laporan polisi maupun permintaan bantuan penyelidikan dari berbagai negara, yang dikirimkan baik melalui *diplomatic channel* maupun *interpol channel*, dengan total kerugian sebesar USD 9,1 juta atau sekitar Rp.126 M,-. Selama periode tahun 2012 sampai dengan bulan Juni tahun 2016, jumlah tindak pidana siber yang dilaporkan sebanyak 7.697 laporan, dengan penyelesaian kasus sebanyak 1.464 laporan, dengan kata lain hanya 19,02% kasus yang dapat diselesaikan.

Dalam melaksanakan tugas pokoknya, Subdirektorat IT & *Cyber Crime* Dit Tipideksus Bareskrim Polri juga dilengkapi Unit Digital Forensik yang merupakan bagian dari proses penyidikan yang tidak terpisahkan dalam mengumpulkan alat bukti digital guna membuat terang tindak pidana yang terjadi serta menemukan tersangkanya. Unit Digital Forensik Subdirektorat IT & *Cyber Crime* Dit Tipideksus Bareskrim Polri juga telah mendapatkan Akreditasi sebagai laboratorium uji sesuai ISO 17025 : 2005 yang diterbitkan oleh Komite Akreditasi Nasional, yang juga merupakan anggota dari *Asia Pacific Accreditation Committee (APAC)*. Sepanjang tahun 2015 Unit Digital Forensik Subdirektorat IT & *Cyber Crime* juga membantu proses pemeriksaan barang bukti digital dari Kewilayahan dengan jumlah total 386 Barang Bukti Digital, sedangkan tahun 2016 sampai dengan bulan Juni, Unit Digital Forensik Subdirektorat IT & *Cyber Crime* membantu proses pemeriksaan barang bukti digital dari kewilayahan dengan jumlah total 806 Barang Bukti Digital Permintaan ini akan semakin meningkat seiring dengan bertambah banyaknya masyarakat pengguna internet di tanah air.

Selama kurun waktu lima tahun terakhir Subdit IT dan *Cyber Crime* Dittipideksus Bareskrim Polri telah melakukan penangkapan terhadap lebih dari seribuan tersangka dan hampir 80 % adalah Warga Negara Asing. Dalam *media release* Interpol Desember 2015 diberitakan bahwa 500 orang berhasil ditangkap pada *Operation First Light* 2015 di 23 negara Asia - Pacific, dari jumlah tersebut Indonesia menyumbangkan angka terbesar dalam penangkapan yaitu sebanyak 245 orang tersangka, dimana 119 diantara jumlah tersebut ditangkap oleh Subdit IT dan *Cyber Crime* Dittipideksus Bareskrim Polri. Produktifitas pengungkapan yang dilakukan tersebut masih berbanding terbalik dengan apa yang dilakukan oleh kepolisian kewilayahan, yang pastinya terdapat pengaduan-pengaduan lain.

Bulan Oktober tahun 2015, Subdit IT *& Cyber Crime* Dittipideksus Bareskrim Polri melakukan kerjasama dengan Europol dan Pemerintah Serbia terkait dengan ekstradisi *NIKOLOV ILIEV DIMITAR*, yang bersangkutan terkait pencurian data nasabah/penggandaan kartu ATM di Bali. Subdit IT *& Cyber Crime* memiliki hubungan kerjasama yang baik dengan *FBI (Federal Bureau of Investigation)* serta *NCA (National Crime Agency).* Salah satu kerjasama antara Subdit IT *& Cyber Crime* Dittipideksus Bareskrim Polri dengan *FBI (Federal Bureau of Investigation)* dalam perkara *email fraud* dimana *FBI (Federal Bureau of Investigation)* membantu melakukan pemeriksaan saksi yang berada di *Milwaukee* dan *Minnesota* tanpa penyidik harus berangkat kesana, dan keterangan saksi tersebut dapat diterima di pengadilan.

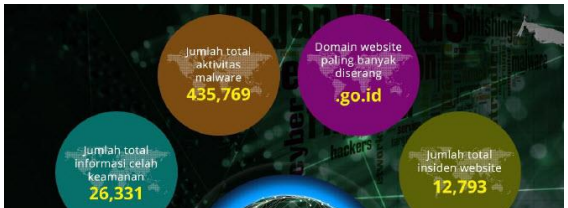
Tindak pidana siber bisa terjadi pada semua sektor, seperti sektor keuangan (perbankan), komunikasi, transportasi dan yang baru-baru ini diungkap oleh penyidik *Cyber crime* Polri adalah serangan terhadap server Lembaga Kebijakan Pengadaan Barang dan Jasa Pemerintah (LKPP), yang dikelola oleh Kementerian Pekerjaan Umum dan Perumahan Rakyat (PUPR), yang mengakibatkan tertundanya lelang pembangunan infrastruktur sebesar 47 T, dan tentunya berpengaruh pada perekonomian dan pembangunan nasional.

sumber : ID-SIRTII – Annual Report 2013

Gambar 3. Pemantauan dan Deteksi Intrusi

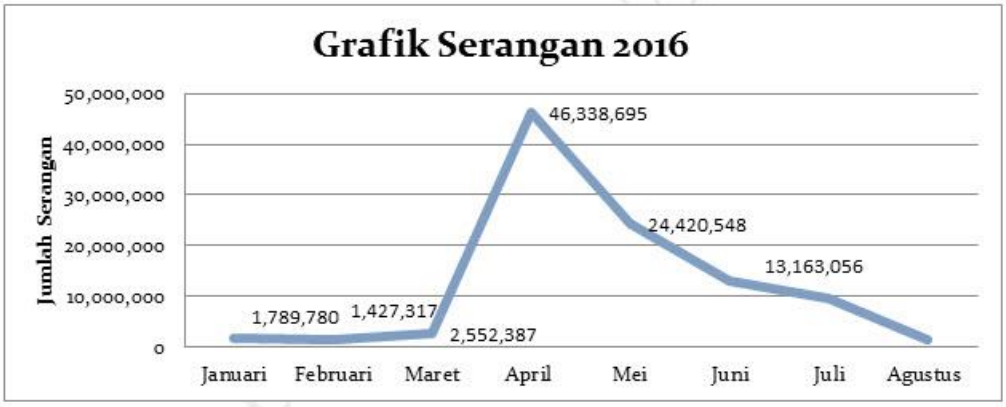
Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) mencatat pada tahun 2013 ada 42 juta serangan, tahun 2014 ada 48,8 juta serangan, dan pada tahun 2015 ada 28 juta serangan *cyber* ke Indonesia. ID-SIRTII mencatat pada tahun 2014, serangan terbanyak diakibatkan oleh adanya aktivitas *"malware"* sejumlah 12.007.808 insiden (*Malware* atau *Malicious Software)* merupakan software atau program yang dirancang bertujuan untuk menyusup atau merusak sebuah sistem komputer secara diam-diam, malware juga dapat dirancang untuk memberikan perintah tertentu pada sistem komputer tanpa diketahui oleh penggunanya. Serangan akibat adanya celah keamanan sebanyak 24.168 kasus, kebocoran rekam jejak atau *"record leakage*" 5.970 kasus.

Ada juga serangan melalui *"password harvesting"* atau *"phising"* (usaha untuk mendapatkan suatu informasi penting dan rahasia secara tidak sah, seperti USER ID, PASSWORD, PIN, informasi rekening bank, informasi kartu kredit, atau informasi rahasia yang lain) sebanyak 1.730 kasus dan serangan akibat kebocoran domain sebanyak 215 kasus. Situs atau Halaman Pemerintah yang beralamat go.id paling banyak mendapat serangan.



Gambar 4. Jumlah Intrusi Trafik

Penurunan serangan pada tahun 2015 tidak memberikan jaminan bahwa *cyberspace* kita sudah aman, hal ini terbukti pada laporan kuartal pertama ID-SIRTII – *Annual Report* 2016, bahwa total serangan pada tahun 2016 sampai dengan bulan Juni adalah sebanyak 89,691,783 kali, dimana serangan terbanyak terjadi pada bulan April sebagaimana grafik berikut :



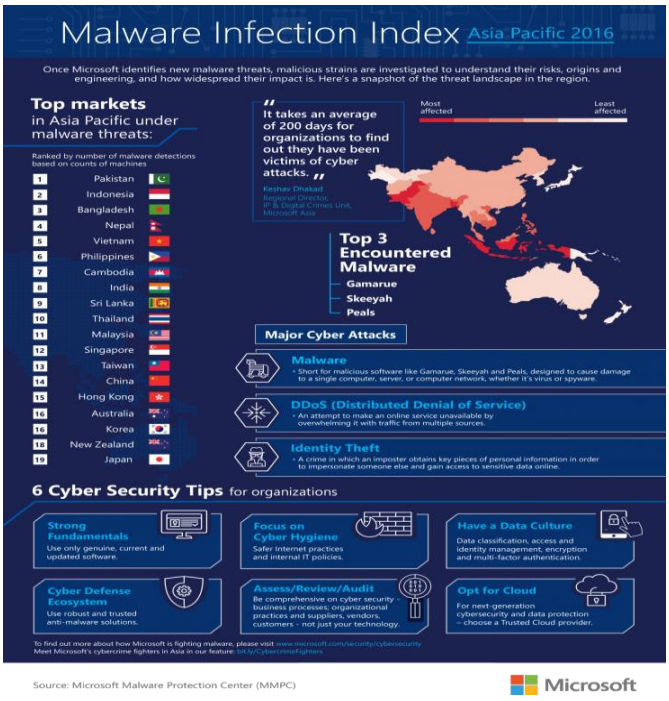
sumber : ID-SIRTII – Annual Report 2016

Gambar 5. Grafik Serangan 2016

Perkembangan teknologi yang memberikan kecenderungan positif terhadap peradaban disatu sisi namun demikian jika tidak dikelola dengan baik, seperti pengelolaan terhadap operator seluler, *internet service provider*, dan *law enforcement* itu sendiri, maka perkembangan teknologi akan banyak dimanfaatkan dalam tindakan-tindakan melawan hukum. Kejahatan apapun

dapat dilakukan di era virtual saat ini baik kejahatan terhadap sistem informasi *(computer crime)* maupun kejahatan lama yang akan lebih mudah dilakukan dengan teknologi informasi *(computer related crime)* dan akan berkontribusi negatif terhadap kehidupan sosial masyarakat, bahkan keamanan negara. Karakteristik kejahatan virtual dilakukan dengan modus-modus anonymous yang memiliki kesulitan tingkat tinggi untuk di identifikasi.

Laporan terkait aktifitas malware pada jaringan internet Indonesia bukan hanya dilaporkan oleh *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII), penelitian Microsoft menempatkan Indonesia pada urutan kedua ancaman malware di wilayah Asia Pasifik sebagaimana artikel yang di terbitkan pada bulan juni tahun 2016 dengan judul *"Malware Infection Index 2016 highlights key threats undermining cybersecurity in Asia Pacific: Microsoft Report"*



Gambar 6. Malware Infection Index

Para kriminal melakukan eksekusi secara trans nasional, terorganisir, tidak pandang bulu termasuk terhadap infra struktur nasional, berdampak masal, bahkan dapat melumpuhkan suatu negara, reputasi serta keamanan publik pada umumnya. Dari data teranyar yang diperlihatkan oleh perusahaan antivirus *Vaksincom*, Indonesia menempati posisi kelima dari 20 besar negara skala

global sebagai korban penyebaran malware *Game Over Zeus* per Maret 2015. Masih dari *Vaksincom*, Indonesia menempati posisi kelima dari 20 besar negara skala global sebagai korban penyebaran malware *Game Over Zeus*, dengan jumlah korban di Indonesia mencapai angka 3.625 per Internet *Protocol (IP) address* dengan persentase 7,37 persen.

Polri sebagai salah satu pilar bangsa yang mendapat otoritas dari konstitusi sebagai aparat penegak hukum, wajib untuk dilakukan *update* terhadap kapabilitas dan kompetensi organisasi sehingga mampu untuk mengaktualisasikan kehadiran negara dalam mencegah, mengantisipasi, dan memerangi kejahatan-kejahatan virtual (*Cyber Crime*) baik *computer related crime,* maupun *computer crime***.** Sehingga Polri memiliki kapasitas untuk dapat menyesuaikan diri dalam menghadapi tantangan peradaban virtual di abad informasi saat ini. Artinya bahwa keberadaan struktur organisasi *cyber* saat ini perlu dievaluasi untuk diperkuat agar dapat beradaptasi dengan peradaban baru. Evaluasi tersebut adalah melakukan *update* terhadap organisasi sehingga mampu menjawab tantangan publik, melalui analisa terhadap: Formalisasi; Sentralisasi; Spesialisasi; Standarisasi; Kompleksitas; Hirarki kekuasaan. Sehingga untuk menjawab kondisi tersebut, maka diperlukan sebuah kajian secara mendalam (penelitian) tentang pengembangan satuan/unit *cyber crime* disatuan kewilayahan (Polda dan Polres)

B. Rumusan Masalah

Bagaimanakah pengembangan struktur organisasi direktorat satuan/unit *cyber crime* di kewilayahan. Berangkat dari rumusan masalah tersebut, maka persoalan yang dikaji adalah sebagai berikut :

a. Seperti apakah struktur organisasi *cyber crime* di tingkat Polda ?
b. Seperti apakah struktur organisasi *cyber crime* di tingkat Polres ?

C. Tujuan dan Manfaat

1. Tujuan

   Untuk melakukan pengembangan/penataan struktur organisasi direktorat satuan/unit *cyber crime* di tingkat Polda dan Polres.

2. Manfaat

Mengantisipasi merebaknya kejahatan *cyber* disemua sektor kehidupan seperti sektor pemerintah, perbankan, industri, politik, dan lain-lain sebagai dampak masivnya perkembangan Teknologi Infomasi Komunikasi yang berimplikasi pada tugas Polri.

D. Ruang Lingkup

Ruang lingkup dalam kajian ini dibatasi pada pengembangan struktur organisasi Direktorat satuan/unit siber di kewilayahan (Polda dan Polres)

E. Sistematika Laporan

BAB I PENDAHULUAN

BAB II KAJIAN TEORI

BAB III METODE KAJIAN

BAB IV ANALISIS HASIL KAJIAN

BAB V KESIMPULAN DAN REKOMENDASI

BAB VI PENUTUP

BAB II
KAJIAN TEORITIK

A. Pengertian Pengembangan Struktur Organisasi

Organisasi dalam arti yang cukup sederhana dapat diartikan alat, bagian atau badan. Menurut Chester I.Barnard, organisasi merupakan suatu susunan skematis yang menggambarkan sistem aktivitas kerjasama. Organisasi dalam arti bagan atau struktur adalah gambaran secara skematis tentang hubungan-hubungan, kerjasama dari orang-orang yang terdapat dalam organisasi dalam rangka usaha mencapai sesuatu tujuan (Manullang,1981: 23). Dalam konteks demikian maka pengertian organisasi dikatakan organisasi statis yang sering disebut juga bagan organisasi, ranji organisasi, skema organisasi atau lebih dikenal struktur organisasi.

Pengembangan organisasi adalah penataan organisasi baik dalam bentuk restrukturisasi ataupun strukturisasi. Agar organisasi dapat berjalan dengan baik atau dalam rangka membentuk suatu organisasi yang efisien dan efektif, ada sejumlah prasyarat yang harus dipenuhi dalam usaha menyusun suatu struktur organisasi. Prasyarat tersebut dalam kajian teoritik organisasi disebut asas-asas atau prinsip-prinsip organisasi, yaitu : perumusan tujuan, pembagian kerja, delegasai kekuasaan, rentang kendali, hirarkhi pengawasan, kestauan perintah dan tanggungjawab, dan koordinasi.

Dalam kerangka pengembangan struktur organisasi *cyber* pada tingkat kewilayahan (Polda dan Polres), ketujuh asas dasar organisasi itu harus dijadikan pertimbangan. Artinya, pembentukan atau pengembangan struktur organisasi harus mengikuti setidaknya 7 (tujuh) prinsip organisasi itu. Permasalahannya adalah struktur organisasi *cyber* di tingkat Mabes dan Polda sudah terbentuk, namun di tingkat Polres belum terbentuk. Dalam perpektif kelembagaan, hal ini merupakan indikator adanya inkonsistensi dalam pengetrapan prinsip-prinsip organisasi yang efisien dan efektif.

Dalam kerangka menciptakan organisasi yang baik, dalam arti efektif dan efisien maka diperlukan kajian pengembangan struktur organisasi cyber crime di tingkat kewilayahan. Menurut konsepsi teoritis, apabila di tingkat Pusat sudah terbentuk struktur organisasi *cyber* maka di tingkat Polda, dan Polres juga perlu dibentuk. Hal ini sesuai dengan asas organisasi, yakni hirarki pengawasan (*span of management).*

Disamping itu pengembangan struktur organisasi juga harus mempertimbangkan salah satu prinsip organisasi, yaitu kesatuan perintah dan tanggungjawab (*unity of command & responsibility*). Menurut prinsip ini seorang bawahan hanya mempunyai seorang atasan dari siapa ia menerima perintah dan kepada siapa ia memberi pertanggungjawaban atas pelaksanaan tugasnya. Motto yang terkenal dari asas ini ialah '*no man can serve two bosses'*.

Oleh karena itu dalam kajian teoritik organisasi tidak dibenarkan, apabila terdapat tugas dan tanggungjawab telah didelegasikan namun secara struktural organisasinya tidak ada. Artinya, tugas dan fungsinya dilaksanakan oleh organisasi atau bagian lain yang bukan bidangnya, bahkan organisasi itu telah memiliki tupoksi sendiri. Apabila hal ini terjadi dalam suatu organisasi maka tingkat efektifitas dan kinerja organisasi akan cenderung rendah. Tingkat efektifitas akan lebih rendah lagi manakala pekerjaan atau tugas itu membutuhkan profesionalisme yang bersifat khusus atau kompetensi khusus, seperti *cyber crime,* dan lain-lain.

B. Pengertian *Cyber Crime*

Kemajuan teknologi telah merubah struktur masyarakat dari yang bersifat lokal menuju ke arah masyarakat yang berstruktur global. Perubahan ini disebabkan oleh kehadiran teknologi informasi. Perkembangan teknologi informasi itu berpadu dengan media dan komputer, yang kemudian melahirkan piranti baru yang disebut internet. Kehadiran internet telah memunculkan paradigma baru dalam kehidupan manusia. Kehidupan berubah dari yang hanya bersifat nyata (real) ke realitas baru yang bersifat maya (Virtual). Realitas yang kedua ini biasa dikaitkan dengan internet dan *cyber space*. Perkembangan Internet yang semakin hari semakin meningkat, baik perangkat maupun penggunaannya, membawa dampak positif atau pun negatif.

Kejahatan dunia maya (Inggris: ***cyber crime***) adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online,

pemalsuan cek, penipuan kartu kredit/carding, confidence fraud, penipuan identitas, pornografi anak, dan lain-lain

Andi Hamzah : dalam bukunya "Aspek-aspek Pidana di Bidang Komputer" (1989) mengartikan ***cyber crime*** sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal.

Forester dan Morrison : mendefinisikan kejahatan komputer sebagai: aksi kriminal dimana komputer digunakan sebagai senjata utama.

Girasa (2002) : mendefinisikan ***cyber crime*** sebagai aksi kejahatan yang menggunakan teknologi komputer sebagai komponen utama.

Tavani (2000) : memberikan definisi ***cyber crime*** yang lebih menarik, yaitu kejahatan dimana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi cyber dan terjadi di dunia cyber.

C. Sejarah dan Perkembangan *Cyber Crime*

1. Sejarah dan Perkembangan *Cyber Crime* di Dunia

   Awal mula penyerangan didunia *Cyber* pada tahun 1988 yang lebih dikenal dengan istilah *Cyber Attack* Pada saat itu ada seorang mahasiswa yang berhasil menciptakan sebuah worm atau virus yang menyerang program computer dan mematikan sekitar 10% dari seluruh jumlah komputer di dunia yang terhubung ke internet.

   Pada tahun 1994 seorang anak sekolah musik yang berusia 16 tahun yang bernama Richard Pryce, atau yang lebih dikenal sebagai *"the hacker"* alias *"Datastream Cowboy",* ditahan lantaran masuk secara ilegal ke dalam ratusan sistem komputer rahasia termasuk pusat data dari Griffits Air Force, NASA dan *Korean Atomic Research Institute* atau badan penelitian atom Korea. Dalam interogasinya dengan FBI, ia mengaku belajar *hacking* dan *cracking* dari seseorang yang dikenalnya lewat internet dan menjadikannya seorang mentor, yang memiliki julukan "Kuji". Hebatnya, hingga saat ini sang mentor pun tidak pernah diketahui keberadaannya. Hingga akhirnya,

pada bulan Februari 1995, giliran Kevin Mitnick diganjar hukuman penjara untuk yang kedua kalinya. Dia dituntut dengan tuduhan telah mencuri sekitar 20.000 nomor kartu kredit! Bahkan, ketika ia bebas, ia menceritakan kondisinya di penjara yang tidak boleh menyentuh komputer atau telepon.

2. Sejarah dan Perkembangan *Cyber Crime* di Dunia

Di Indonesia sendiri juga sebenarnya prestasi dalam bidang *cyber crime* ini patut diacungi dua jempol. Walau di dunia nyata kita dianggap sebagai salah satu negara terbelakang, namun prestasi yang sangat gemilang telah berhasil ditorehkan oleh para *hacker, cracker* dan *carder* lokal. Virus komputer yang dulunya banyak diproduksi di US dan Eropa sepertinya juga mengalami *"outsourcing"* dan globalisasi. Di tahun 1986 – 2003, epicenter virus computer dideteksi kebanyakan berasal dari Eropa dan Amerika dan beberapa negara lainnya seperti Jepang, Australia, dan India. Namun hasil penelitian mengatakan di beberapa tahun mendatang Mexico, India dan Afrika yang akan menjadi *epicenter* virus terbesar di dunia, dan juga bayangkan, Indonesia juga termasuk dalam 10 besar.

Seterusnya 5 tahun belakangan ini China , Eropa, dan Brazil yang meneruskan perkembangan virus-virus yang saat ini mengancam komputer kita semua dan tidak akan lama lagi Indonesia akan dikenal Negara penghasil *hacker, cracker*, nama yang kurang bagus, alasannya, mungkin pemerintah kurang ketat dalam pengontrolan dalam dunia *cyber,* terus terang para hacker di Amerika tidak akan berani untuk bergerak karena pengaturan yang ketat dan system kontrol yang lebih *high-tech* lagi yang dipunyai pemerintah Amerika Serikat.

D. Karakteristik *Cyber Crime*

1. Dalam perkembangannya kejahatan konvensional *cyber crime* dikenal dengan :
   a. Kejahatan kerah biru
   b. Kejahatan kerah putih

2. *Cyber crime* memiliki karakteristik unik yaitu :

a. Ruang lingkup kejahatan.
b. Sifat kejahatan.
c. Pelaku kejahatan.
d. Modus kejahatan.
e. Jenis kerugian yang ditimbulkan.

3. Dari beberapa karakteristik diatas, untuk mempermudah penanganannya maka *cyber crime* diklasifikasikan :

a. ***Cyberpiracy :***

Penggunaan teknologi komputer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer.

b. ***Cybertrespass :***

Penggunaan teknologi komputer untuk meningkatkan akses pada system computer suatu organisasi atau individu.

c. ***Cybervandalism :***

Penggunaan teknologi komputer untuk membuat program yang menganggu proses transmisi elektronik, dan menghancurkan data di komputer.

4. Berdasarkan beberapa literatur serta fakta empiris, *cyber crime* memiliki beberapa karakteristik, yaitu :

a. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etik tersebut terjadi dalam ruang/wilayah siber/*cyber (cyberspace),* sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.
b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet.
c. Perbuatan yang mengakibatkan kerugian materiil maupun immateriil (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasian informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.

e. Perbuatan tersebut sering dilakukan secara transnasional/melintasi batas negara.

E. Hukum Siber *(Cyber Law)*

Undang-undang Informasi dan Transaksi Elektronik atau Undang Undang nomor 11 tahun 2008 atau UU ITE adalah UU yang mengatur tentang informasi serta transaksi elektronik, atau teknologi informasi secara umum. UU ini memiliki yurisdiksi yang berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

1. Definisi :
   a. Pasal 1 Angka 1:

      Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange (EDI),* surat elektronik *(electronic mail),* telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

   b. Pasal 1 Angka 4:

      Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

2. Barang Bukti

a. Pasal 5 Ayat (1):

Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan ALAT BUKTI HUKUM YANG SAH.

b. Pasal 5 Ayat (2):

Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

3. Saksi Ahli

Penjelasan Pasal 43 Ayat (5) Huruf h

Yang dimaksud dengan “ahli” adalah seseorang yang memiliki keahlian khusus di bidang Teknologi Informasi yang dapat dipertanggungjawabkan secara akademis maupun praktis mengenai pengetahuannya tersebut.

4. Pelanggaran

a. Pasal 30

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik:

1) milik orang lain dengan cara apa pun.
2) dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
3) dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

b. Pasal 46

1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.600.000.000,00 (enam ratus juta rupiah).

2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).

c. Pasal 32
1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik.
2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak.
3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

d. Pasal 48
1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp.2.000.000.000,00 (dua miliar rupiah).
2) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp.3.000.000.000,00 (tiga miliar rupiah).

3) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.5.000.000.000,00 (lima miliar rupiah).

e. Pasal 33

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

f. Pasal 49

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.10.000.000.000,00 (sepuluh miliar rupiah).

BAB III
METODE KAJIAN

A. Sampling dan Narasumber/Informan

Penelitian ini merupakan kajian tentang pengembangan organisasi satuan/unit *cyber crime* di satuan kewilayahan (Polda dan Polres), adapun sampel dan narasumbernya sebagai berikut:

1. Narasumber

Narasumber/informan dalam kajian ini adalah pejabat dan personel Subdit *cyber crime* Polri yang bertugas di Polda, pejabat Satuan Reserse kriminal Polres, Kapolsek dan satuan unit serse tingkat Polres dan Polsek

2. Teknik Sampling

Dalam kajian ini teknik pengambilan sampling menggunakan pendekatan *purposive sampling* yakni, sampel telah ditentukan dengan tujuan penelitian. Adapun sebagai sampelnya adalah Polda Metro Jaya,

dan Polda Jatim sudah memiliki struktur organisasi *cyber crime* berbentuk Subdit dibawah kendali Ditkrimsus dan memiliki Laboratorium CCISO sedangkan Polda Banten dan Polda Jawa Barat baru memiliki struktur organisasi *cyber crime* berbentuk Unit dibawah kendali Subdit Mondev Ditkrimsus dan belum memiliki Laboratorium CCISO. Adapun rincian sampelnya dijelaskan pada tabel di bawah ini :

Tabel 1
Sampel Pengkajian

Sampel Polda	Sampel Polres
Polda Metro Jaya	Subdit IV Cyber Crime Polda
	Polres Metro Jakarta Barat
	Polres Kota Depok
	Polres Metro Jakarta Pusat
	Polres Metro Bekasi Kota
	Polres Metro Tangerang Kota
	Polres Tangerang Selatan

Sampel Polda	Sampel Polres
Polda Banten	SUDBIT IV CYBER CRIME POLDA
	POLRES SERANG
	POLRES CILEGON
	POLRES PANDEGLANG
	POLRES LEBAK
	POLRES TANGERANG
Polda Jawa Barat	UNIT CYBER CRIME POLDA
	POLRESTABES BANDUNG
	POLRES TASIK
	POLRES CIAMIS
	POLRES KUNINGAN
	POLRES CIREBON
	POLRES INDRAMAYU
	POLRES SUBANG
Polda Jawa Timur	SUDBIT IV CYBER CRIME POLDA
	POLRESTA SIDOARJO
	POLRESTA PROBOLINGGO
	POLRES PROBOLINGGO
	POLRES SITUBONDO
	POLRES BONDOWOSO
	POLRES JEMBER
	POLRES LUMAJANG
	POLRESTA PASURUAN
	POLRES PASURUAN
	POLRESTA MALANG

	POLRES MALANG
	POLRES BATU

B. Metode Pengumpulan Data

Data yang dikumpulkan terdiri atas

1. Data primer, data hasil diskusi dan wawancara, dengan para narasumber/informan terkait dengan :
   a. Desain struktur *cyber crime* di tingkat Polda dan Polres serta mekanisme kerjanya
   b. Efektivitas kinerja organisasi *cyber crime* di tingkat kewilayahan (SOP, anggaran, Laboratorium, harwat peralatan)
   c. Beban tugas organisasi *cyber crime* dalam mengungkap kasus-kasus kejahatan *cyber crime (computer crime, related crime dan cyber fraud and phising)*
   d. Kemampuan unit *cyber crime* di tingkat kewilayahan (jumlah personel, tingkat pengetahuan, kemampuan penyidik *cyber*, sertifikasi penyidik *cyber* serta sarana prasarana)
   e. Hubungan tata cara kerja dan regulasi dalam aksesibilitas data eksternal untuk pengungkapan kasus kejahatan *cyber crime*

2. Data sekunder,

   Diperoleh dari Polda (Subdit *cyber crime*), Polres (Satkrimsus), tentang jumlah dan bentuk-bentuk kejahatan cyber pada kurun waktu 2015 – 2018, sertifikasi dan standarisasi peralatan Lab, sertifikasi analisis dan penyidik *cyber*

3. Observasi

   Mengamati dan melihat secara langsung penggelaran Laboratorium, peralatan dan tata ruang Subdit *cyber crime*

C. Analisis Data

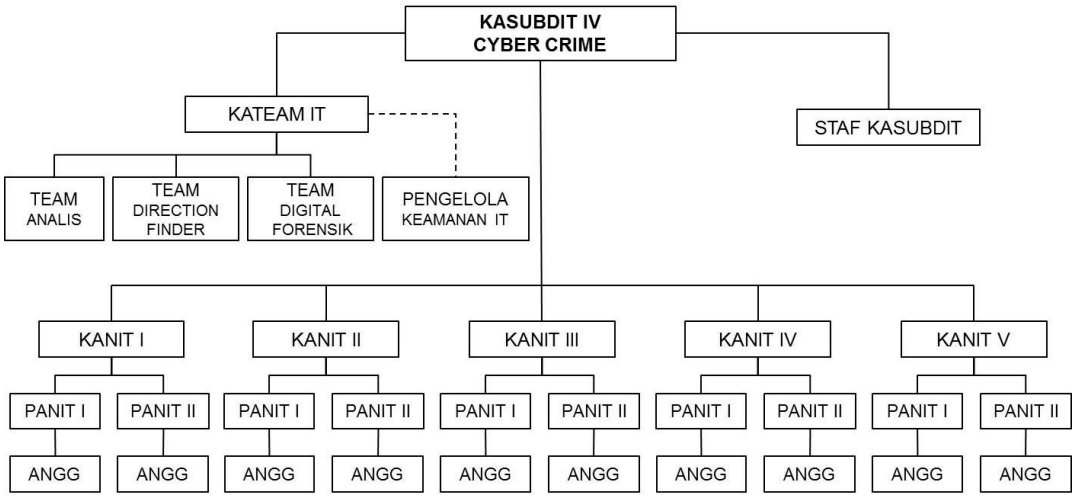
Analisis data yang digunakan dalam mengkaji struktur organisasi *cyber crime* di tingkat kewilayahan (Polda dan Polres) adalah Analisis deskriptif

kualitatif, hal ini dilakukan untuk menentukan model atau bentuk organisasi *cyber crime* di tingkat Polda dan Polres

BAB IV
ANALISIS HASIL PENELITIAN

A. Deskripsi Satuan Organisasi Cyber di Tingkat Polda

1. Struktur Organisasi Cyber Polda Metro Jaya



Gambar 7. Struktur Organisasi Subdit IV cyber crime
Direktorat Reserse Kriminal Khusus Polda Metro Jaya

Berdasarkan penelitian lapangan ditemukan bahwa struktur organisasi *cyber crime* di Polda Metro Jaya statusnya pada leveling Subdirektorat, artinya kedudukan struktur organisasi *cyber crime* dibawah kendali Direktorat Kriminal Khusus (Krimsus) sebagai Subdit IV. Kepala Subdit IV *cyber crime* membawahi V Unit dan Kepala Team IT. Team IT dalam melaksanakan tugas siber dibantu oleh *Team Analis, Team Direction Finder, dan Team Digital Forensik*. Kedudukan struktur organisasi *cyber* di tingkat Polda Metro Jaya seperti itu sudah sesuai dengan amanat

Perkap Nomor 23 Tahun 2010 tentang Struktur Organisasi Tata Kerja Polri. Jadi SOTK di Polda Metro Jaya merupakan implementasi Perkap Kapolri Nomor 23 Tahun 2010.

Gambaran yang ditunjukkan sebgaimana bagan organisasi di atas mendeskripsikan tugas dan wewenang, tanggung jawab, pola hubungan antara fungsi-fungsi, bagian-bagian atau posisi-posisi, rantai perintah dan kesatuan perintah, tingkat hirarki atau komando, dan saluran komunikasi. Struktur organisasi tersebut telah menunjukkan kerangka dan susunan pola tetap hubungan tata kerja dalam organisasi Polda Metro Jaya. HaL ini sekaligus menunjukkan gambaran kekuatan organisasi yang mnengemban tugas pokok dan fungsi *cyber crime* di Polda Metro Jaya. Satuan organisasi *cyber crime* tercermin dari struktur organisasi tersebut, kedudukan organisasinya berstatus sebagai Subdit *Cyber Crime* (Subdit IV Direktorat Kriminal Khsusus), memiliki 5 (lima) Kepala Unit dan 'dibackup' oleh Tim IT yang terdiri dari *tim analysis*, *tim direction finder, tim digital forensic*, dan tim keamanan IT.

Berangkat dari struktur organisasi di atas maka tugas-tugas yang diemban oleh subdit cyber crime, yaitu :

a. Penyidikan kasus-kasus yang berhubungan dengan transaksi elektronik, money loundring, pasar modal, pajak, perbankan, dll)
b. Penyidikan kasus-kasus yang berhubungan dengan teknologi komunikasi dan informasi (penyadapan telepon, penyalahgunaan Voip, penipuan melalui telepon genggam)
c. Penyelidikan kejahatan yang menggunakan fasilitas Internet (*cyber gambling, cyber terrorism, cyber fraud, cyber sex, cyber narcotism, cyber smuggling, cyber attacks on critical infrastructure, cyber black mail, cyber theatening*, pencurian data, pencemaran nama baik, dll)
d. Penyidikan kejahatan computer (masuk ke system secara illegal, *ddos atack, hacking, tracking, phreacing*, membuat dan menyebarkan yang bersifat merusak seperti *malicous code al viruses, worm, rabbits trojan*, dll)

e. Penyidikan kejahatan yang berhubungan dengan Hak atas Intelektual (Pirated Software, rekaman suara, merubah tampilan website)

Adapun kekuatan dan kemampuan peronel satuan organisasi *Cyber Crime* di Polda Metro Jaya, yaitu sebanyak 76 orang. Apabila dilihat dari aspek kualitas penyidik, kekuatan dan kemampuan penyidik siber Polda Jaya telah memiliki hanya 4 orang yang memiliki sertifikasi program *Certified Ethical Hacker (CEH)* dan memiliki sertifikasi program *Computer Hacking Forensic Investigator Certification* (CHFI) untuk melakukan pemeriksaan barang bukti digital laboratorium digital forensic.Sedangkan yang 3 orang penyidik lainnya belum memilki sertifikat internasional namun kemampuannya relative memadai dalam bidang *cyber crime.*

Jumlah personel *cyber crime* tersebut terdistribusi menurut penempatan dan jabatan masing-masing, yaitu :

a. Kasubdit Cyber 1 personel
b. Tim analis 2 personel
c. Tim Survailance 5 personel
d. Tim Direction Finder 6 personel
e. Tim IT support 1 personel
f. Tim Lab forensik 7 personel
g. Unit Lidik Sidik 54 personel

Dengan kekuatan personel di atas jumlah kasus yang ditangani perhari kurang lebih 20 - 30 kasus, sehingga bila dirata-rata kasus yang ditangani perbulan mencapai 700 - 900 kasus. Selain itu ada tambahan tugas kasus-kasus prioritas yang perlu penanganan khusus dan cepat, seperti; kasus cyber yang berskala “Prioritas” bagi para pejabat negara setingkat Menteri termasuk (RI 1/RI 2, TB1 dan TB2) yang selalu menjadi atensi pimpinan Polri, dan tambahan kasus cyber yang tidak mampu ditangani oleh Badan Intelejen Nasional (BIN).

Disamping itu Polda Metro Jaya memiliki kekuatan organisasi cukup memadai apabila dilihat dari aspek sarana dan prasarana dalam penanganan kasus-kasus *cyber crime.* Polda Metro Jaya memiliki laboratorium cukup lengkap dibanding Polda lainnya, Laboratorium dan

sarana lain dalam penegakan hukum siber menjadi factor penting satuan/organisasi *cyber crime* karena sarana-prasarana dan laboratorium merupakan instrument utama dalam pengungkapan kasus dan penegakan hukum kejahatan siber *(cyber law).*

Laboratorium *cyber crime* yang dimiliki di Polda Metro Jaya, yaitu *Cyber Crime Investigation Satelit Office* (CCISO) yang terdiri :

a. Laboratorium Komputer Forensik
b. Laboratorium Mobile Phone Forensik
c. Laboratorium Audio Video Forensik

Selain itu Polda Metro Jaya memiliki laboratorium *Strategic Informasi and Tactical Operation Centre* (SITOC) yang terdiri :

a. Laboratorium Analisis Komunikasi
b. Laboratorium Analisis Keuangan
c. Laboratorium Command Center

Selain itu Laboratorium *cyber crime* yang dimiliki di Polda Metro Jaya, yaitu *Cyber Crime Investigation Satelit Office* (CCISO) yang terdiri :

a. Laboratorium Komputer Forensik
b. Laboratorium Mobile Phone Forensik
c. Laboratorium Audio Video Forensik

Adapun peralatan lain yang dimiliki Polda Metro Jaya, yaitu *mobile direction finder, Cellebrite, check post, CDR,* dan lain-lain. Semua peralatan dan laboratorium di atas sudah ditera dan diakreditasi. Sarana prasarana, yakni fasilitas pemeriksaan barang bukti digital (Lab Digital Forensik)

Disamping itu Subdit Tindak Pidana Siber telah memiliki Akreditasi KAN SNI ISO 17025:2008, hal ini merupakan bukti sekaligus pengakuan bahwa prosedur yang dilaksanakan telah memenuhi standar internasional sebuah laboratorium uji. Namun masih ada kelemahan karena tempt penyimpanan ruang barang bukti digital forensic, seperti *computer, handphone, laptop, note book, tabled,* dll. masih belum cukup.

Fasilitas lain yang dimiliki Polda Metro Jaya ialah *"Monitoring Center"* yang terkait dengan monitoring media social, karena semakin meningkatnya jumlah pengguna internet dan media sosial di Indonesia. Subdit Tindak Pidana Siber dituntut untuk mengikuti perkembangan informasi, teknologi dan komunikasi salah satunya Polda harus memiliki fasilitas 'monitoring center'. Kebutuhan ini kini semakin mendesak, terkait dengan maraknya media sosial, hoax, ujaran kebencian, penipuan on line dan sebagainya.

Fasilitas monitoring center merupakan pendukung dalam penegakan hukum siber yang lebih professional, modern, dan terpercaya. Fasilitas "*Monitoring Center*" sebagai cyber patrol media sosial dapat dikembangkan untuk membantu memperlancar penanganan kasus tindak pidana Siber berkaitan dengan Pilpres Tahun 2019, Pemilu serentak, dan sebagainya.

2. Struktur Organisasi Cyber Polda Jawa Barat

Gambar 8. Struktur Organisasi Dit Reskrimsus Polda Jawa Barat

Berdasarkan penelitian lapangan ditemukan bahwa struktur organisasi *cyber crime* di Polda Jawa Barat statusnya masih pada leveling Unit dibawah kendali Subdirektorat di Direktorat Kriminal Khusus, artinya

kedudukan struktur organisasi *cyber crime* dibawah kendali Subdit Perbankan, Pencucian Uang dan Kejahatan Dunia Maya. Kepala Subdit tersebut salah satunya membawahi Kepala Unit Pencucian Uang dan Dunia Maya.

Jadi, kedudukan struktur organisasi yang mengemban tugas *cyber crime* di Polda Jabar masih dibawah kendali Kepala Unit Subdit, kedudukan organisasi *cyber crime* belum berbentuk Subdit *cyber crime.* Kedudukan satuan organisasi *cyber crime* di tingkat Polda seharusnya merupakan implementasi Perkap Kapolri Nomor 23 Tahun 2010. Namun di Polda Jabar belum seperti itu karena kekurangan sumberdaya yang ada dan kasus-kasus kejahatan siber masih dapat ditangani oleh organisasi setingkat Unit *cyber crime.*

Gambaran yang ditunjukkan sebagaimana bagan organisasi di atas mendeskripsikan tugas dan wewenang, tanggungjawab, pola hubungan antara fungsi-fungsi, bagian-bagian atau posisi-posisi, rantai perintah dan kesatuan perintah, tingkat hirarki atau komando, dan saluran komunikasi. Disamping itu struktur organisasi tersebut telah menunjukkan kerangka dan susunan pola tetap hubungan tata kerja dalam organisasi Polda Jawa Barat. Hal ini sekaligus menunjukkan gambaran kekuatan organisasi yang mengemban tugas pokok dan fungsi *cyber crime* di Polda Jabar.

Dengan demikian kekuatan organisasi *cyber crime* di Polda Polda Jawa Barat dengan sendirinya tercermin dari struktur organisasi tersebut, yakni kedudukan organisasinya berstatus setingkat Unit Organisasi. Dalam melaksanakan tugasnya Kepala Unit *cyber* dibantu oleh personel IT, Tim Survailance, Tim Lab Forensik, dan Unit Lidik Sidik. Adapun tugas yang diemban Unit cyber crime tergambar sebagaimana tugas direktorat krimsus seperti dibawah ini sbb. :

a. Penyidikan kasus-kasus yang berhubungan dengan transaksi elektronik, money loundring, pasar modal, pajak, perbankan, dll)

b. Penyidikan kasus-kasus yang berhubungan dengan teknologi komunikasi dan informasi (penyadapan telepon, penyalahgunaan Voip, penipuan melalui telepon genggam).
c. Penyelidikan kejahatan yang menggunakan fasilitas Internet (*cyber gambling, cyber terrorism, cyber fraud, cyber sex, cyber narcotism, cyber smuggling, cyber attacks on critical infrastructure, cyber black mail, cyber theatening*, pencurian data, pencemaran nama baik, dll).
d. Penyidikan kejahatan computer (masuk ke system secara illegal, *ddos atack, hacking, tracking, phreacing*, membuat dan menyebarkan yang bersifat merusak seperti *malicous code al viruses, worm, rabbits trojan*, dll).
e. Penyidikan kejahatan yang berhubungan dengan Hak atas Intelektual (Pirated Software, rekaman suara, merubah tampilan website).

Apabila dilihat dari aspek kekuatan dan kemampuan satuan organisasi Unit *cyber crime* Polda Jabar hanya memiliki sebanyak 14 personel yang bertugas di unit cyber crime, dari 14 orang tersebut belum ada yang memiliki sertifikasi program *Certified Ethical Hacker (CEH)* dan sertifikasi program *Computer Hacking Forensic Investigator Certification* (CHFI) untuk melakukan pemeriksaan barang bukti digital di laboratorium digital forensic.

Keempat belas tersebut menduduki tugas masing-masing yaitu :

a. Unit Cyber 1 personel
b. Tim Analis 2 personel
c. Tim Survailance 2 personel
d. Tim Lab Forensik 2 personel
e. Unit Lidik Sidik 7 personel

Sedangkan bila dilihat dari aspek peralatan/laboratorium cyber crime, Polda Jabar belum memiliki laboratorium *Cyber Crime Investigation Satelit Office* (CCISO) yang terdiri :

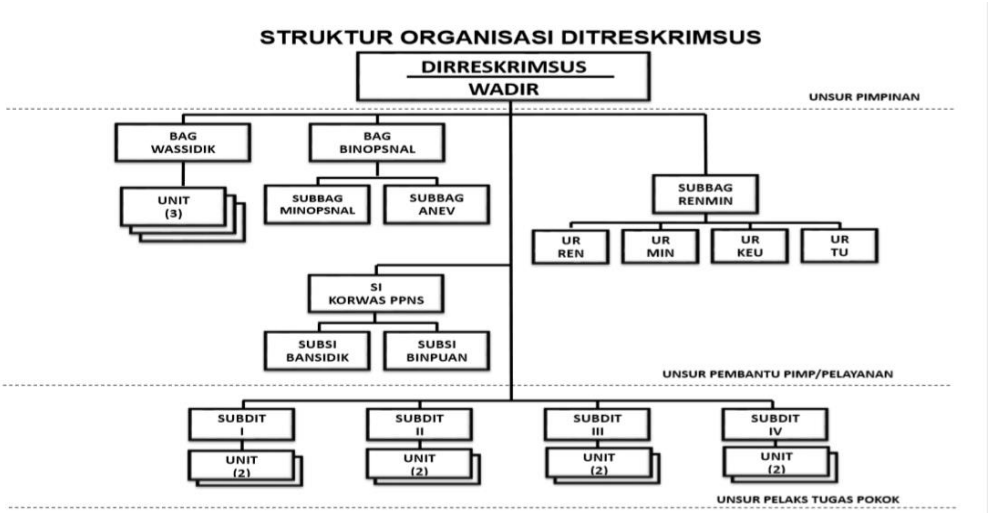
a. Laboratorium Komputer Forensik
b. Laboratorium Mobile Phone Forensik
c. Laboratorium Audio Video Forensik

Selain itu Polda Jabar juga belum memiliki Laboratorium *Strategic Informasi and Tactical Operation Centre* (SITOC) yang terdiri :

a. Laboratorium Analisis komunikasi
b. Laboratorium Analisis Keuangan
c. Laboratorium command center

Sarana-prasarana unit cyber crime juga relative terbatas, sehingga tidak jarang meminjam peralatan dari Direktorat Narkoba dan Kriminal Umum. Dalam penelitian lapangan ditemukan antara lain ruang penyimpanan alat bukti digital, seperti computer, hardisk, laptop, handphone, tablet, dll. belum memadai. Demikian pula fasilitas lain, seperti laboratorium digital/forensik, anlisa komunikasi, monitoring center dll.

3. Struktur Organisasi Cyber Polda Banten



Gambar 9. Struktur Organisasi Dit Reskrimsus Polda Banten

Berdasarkan penelitian lapangan ditemukan bahwa struktur organisasi *cyber crime* di Polda Banten statusnya masih pada leveling Unit dibawah kendali Subdirektorat di Direktorat Kriminal Khusus, artinya kedudukan struktur organisasi cyber crime dibawah kendali Subdit Perbankan, Pencucian Uang dan Kejahatan Dunia Maya. Kepala Subdit tersebut salah satunya membawahi Kepala Unit Pencucian Uang dan Dunia Maya.

Jadi, kedudukan struktur organisasi yang mengemban tugas *cyber crime* di Polda Banten masih dibawah kendali Kepala Unit Subdit, kedudukan organisasi *cyber crime* belum berbentuk Subdit *cyber crime.* Kedudukan satuan organisasi *cyber crime* di tingkat Polda seharusnya merupakan implementasi Perkap Kapolri Nomor 23 Tahun 2010. Namun di Polda Banten belum seperti itu karena kekurangan sumberdaya yang ada dan kasus-kasus kejahatan siber masih dapat ditangani oleh organisasi setingkat Unit *cyber crime.*

Gambaran yang ditunjukkan sebagaimana bagan organisasi di atas mendeskripsikan tugas dan wewenang, tanggungjawab, pola hubungan antara fungsi-fungsi, bagian-bagian atau posisi-posisi, rantai perintah dan kesatuan perintah, tingkat hirarki atau komando, dan saluran komunikasi. Disamping itu struktur organisasi tersebut telah menunjukkan kerangka dan susunan pola tetap hubungan tata kerja dalam organisasi Polda Jawa Banten. Hal ini sekaligus menunjukkan gambaran kekuatan organisasi yang mengemban tugas pokok dan fungsi *cyber crime* di Polda Banten.

Dengan demikian kekuatan dan kemam[uan organisasi *cyber crime* di Polda Polda Banten dengan sendirinya tercermin dari struktur organisasi tersebut, yakni kedudukan organisasinya berstatus setingkat Unit Organisasi. Dalam melaksanakan tugasnya Kepala Unit *Cyber* dibantu oleh personel IT, Tim Survailance, Tim Lab Forensik, dan Unit Lidik Sidik.

Sedangkan apabila dilihat dari aspek peralatan/laboratorium *cyber crime*, Polda Banten belum memiliki laboratorium *Cyber Crime Investigation Satelit Office* (CCISO) yang terdiri :

a. Laboratorium Komputer Forensik
b. Laboratorium Mobile Phone Forensik
c. Laboratorium Audio Video Forensik

Selain itu Polda Banten juga belum memiliki Laboratorium *Strategic Informasi and Tactical Operation Centre* (SITOC) yang terdiri :

a. Laboratorium Analisis komunikasi

b. Laboratorium Analisis Keuangan

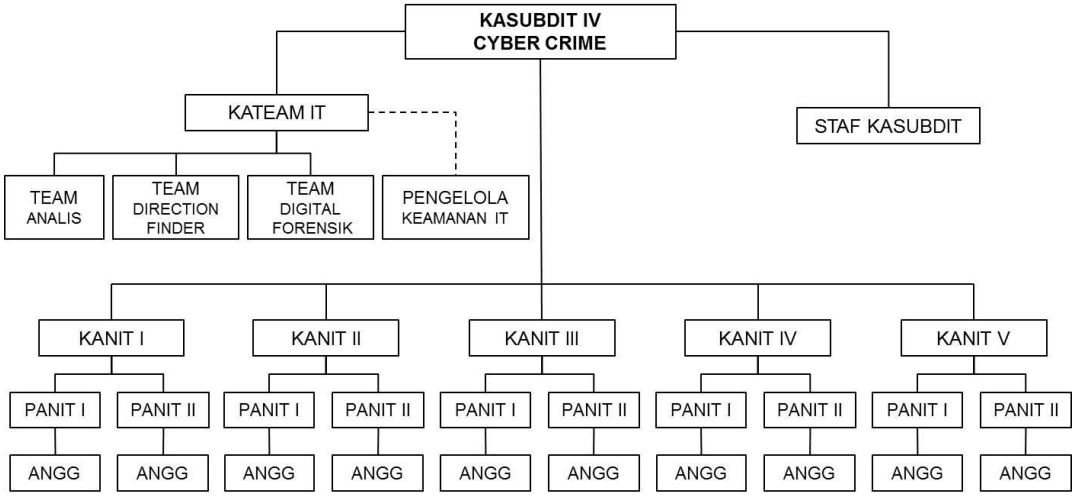
c. Laboratorium command center

Sarana-prasarana unit *cyber crime* juga relative terbatas, sehingga tidak jarang meminjam peralatan dari Direktorat Narkoba dan Kriminal Umum. Dalam penelitian lapangan ditemukan antara lain ruang penyimpanan alat bukti digital, seperti computer, hardisk, laptop, handphone, tablet, dll. belum memadai. Demikian pula fasilitas lain, seperti laboratorium digital/forensik, anlisa komunikasi, monitoring center dll.

Jumlah personel dan penyidik *cyber crime* Polda Banten masih kurang memadai bila dibandingkan dengan beban tugas dan tanggungjwab personel. Sementara dilihat dari segi kualitas, mereka belum memiliki certificate internasional yang mengemban tugas *cyber crime* bahkan sertifikat bertaraf nasional juga belum. Pada hal persyaratan penyidik *cyber crime* salah satunya harus mempunyai sertifikat internasional seperti ; sertifikasi program *Certified Ethical Hacker (CEH)* dan sertifikat program *Computer Hacking Forensic Investigator Certification* (CHFI) untuk melakukan pemeriksaan barang bukti digital laboratorium digital forensic.

Jadi kemampuan personel dari segi kualitas masih kurang karena belum memiliki sertifikat tersebut, mereka juga belum mengikuti pendidikan kejuruan (dikjur) *cyber crime* dan kursus atau diklat *cyber crime.* Personel yang bertugas di satuan *cyber crime* kebanyakan belajar mandiri dan atas biaya sendiri.

4. Struktur Organisasi Cyber Polda Jawa Timur



Gambar 10. Struktur Organisasi Subdit *cyber crime*
Direktorat Reserse Kriminal Khusus Polda Jawa Timur

Berdasarkan penelitian lapangan ditemukan bahwa struktur organisasi cyber crime di Polda Jawa Timur statusnya pada leveling Subdirektorat, artinya kedudukan struktur organisasi *cyber crime* dibawah kendali Direktorat Kriminal Khusus (Krimsus) sebagai Subdit IV. Kepala Subdit IV *cyber crime* membawahi V Unit dan Kepala Team IT. Team IT dalam melaksanakan tugas siber dibantu oleh Team Analis, Team Direction Finder, dan Team Digital Forensik.

Kedudukan struktur organisasi *cyber* di tingkat Polda Jawa Timur semacam itu sudah sesuai dengan amanat Perkap Nomor 23 Tahun 2010 tentang Struktur Organisasi Tata Kerja Polri. Jadi di Polda Jatim SOTK-nya sudah sesuai dengan Peraturan Kapolri Nomor 23 Tahun 2010. Artinya, kedudukan organisasi satuan *cyber crime* di Polda Jawa Timur dibawah kendali Direktorat Kriminal Khusus, yakni berbentuk Sub Direktorat di Direktorat Kriminal Khusus (Subdit *Cyber Crime*).

Gambaran yang ditunjukkan sebgaimana pada bagan organisasi di atas mendeskripsikan tugas dan wewenang, tanggungjawab, pola hubungan antara fungsi-fungsi, bagian-bagian atau posisi-posisi, rantai perintah dan kesatuan perintah, tingkat hirarki atau komando, dan saluran

komunikasi. Struktur organisasi tersebut telah menunjukkan kerangka dan susunan pola tetap hubungan tata kerja dalam organisasi Polda Jatim. Kondisi itu sekaligus menunjukkan gambaran kekuatan dan kemampuan organisasi yang mengemban tugas pokok dan fungsi *cyber crime* di Polda Jatim.

Satuan organisasi *cyber crime* tercermin dari struktur organisasi tersebut, kedudukan organisasinya berstatus sebagai Subdit *cyber crime* (Subdit IV Direktorat Kriminal Khsusus), memiliki 5 (lima) Kepala Unit dan 'dibackup' oleh Tim IT yang terdiri dari *tim analysis*, *tim direction finder, tim digital forensic*, dan tim keamanan IT.

Berangkat dari struktur organisasi di atas maka tugas-tugas yang diemban oleh subdit cyber crime, yaitu :

a. Penyidikan kasus-kasus yang berhubungan dengan transaksi elektronik, money loundring, pasar modal, pajak, perbankan, dll)
b. Penyidikan kasus-kasus yang berhubungan dengan teknologi komunikasi dan informasi (penyadapan telepon, penyalahgunaan Voip, penipuan melalui telepon genggam)
c. Penyelidikan kejahatan yang menggunakan fasilitas Internet (*cyber gambling, cyber terrorism, cyber fraud, cyber sex, cyber narcotism, cyber smuggling, cyber attacks on critical infrastructure, cyber black mail, cyber theatening*, pencurian data, pencemaran nama baik, dll)
d. Penyidikan kejahatan computer (masuk ke system secara illegal, *ddos atack, hacking, tracking, phreacing*, membuat dan menyebarkan yang bersifat merusak seperti *malicous code al viruses, worm, rabbits trojan*, dll).
e. Penyidikan kejahatan yang berhubungan dengan Hak atas Intelektual (Pirated Software, rekaman suara, merubah tampilan website)

Dari aspek peralatan dan laboratorium Polda Jawa Timur telah memiliki laboratorium *Cyber Crime Investigation Satelit Office* (CCISO) yang terdiri :

a. Laboratorium Komputer Forensik

b. Laboratorium Mobile Phone Forensik
c. Laboratorium Audio Video Forensik

Adapun peralatan lain yang dimiliki Polda Jawa Timur, yaitu *cellebrite, check post,* dan lain-lain. Apabila dilihat dari segi peralatan untuk mengungkap suatu kasus-kasus kejahatan siber, kemampuan peralatannya (material) cukup memadai sebab memiliki *mobile direction finder* (DF) 3 (tiga) unit. Jumlah personel Subdit *Cyber crime* sebanyak 68 orang, tetapi dilihat dari standarisasi dan sertifikasi penyidik *cyber,* jumlah penyidik *cyber* Polda Jawa Timur relalif terbatas.

Penyidik yang memiliki sertifikasi program *Certified Ethical Hacker (CEH)* dan memiliki sertifikasi program *Computer Hacking Forensic Investigator Certification* (CHFI) masih sedikit untuk melakukan pemeriksaan dan penyidikan barang bukti digital laboratorium dan digital forensic. Namun beberapa penyidik sudah memiliki kualifikasi internasional walaupun belum bersertifikat Internasional.

Kemampuan penyidik dalam menangani kasus-kasus cyber cukup memadai, seperti :
a. Kemampuan Bahasa Inggris
b. Kemampuan Komputer Forensik
c. Kemampuan Mobile Forensik
d. Kemampuan Analisis jaringan transaksi keuangan dan komunikasi
e. Kemampuan *cyber law*

Akan tetapi kekuatan dan kemampuan organisasi cyber belum optimal karena salah satunya berkaitan dengan sarana-prasarana Markas Komando Subdit Cyber kurang memadai. Contohnya, ruang laboratorium dan ruang penyimpanan alat bukti, seperti computer, hardisk, laptop, handphone, tablet, terlalu kecil dengan tata ruang kurang nyaman. Demikian pula fasilitas lain, seperti laboratorium digital/forensik, analisa komunikasi, monitoring center dll.

B. Struktur Organisasi Cyber di Tingkat Polres

Gambar 11. Struktur Organisasi Sat Reskrim Polres

Berdasarkan hasil penelitian lapangan diperoleh data dan informasi bahwa struktur organisasi cyber crime di tingkat Polres tidak ada. Di polres-polres yang menjadi sampling penelitian tidak ditemukan bentuk organisasi formal yang menangani kasus kejahatan siber, kecuali di Polres Metro Jakarta Barat ditemukan unit organisasi cyber crime dibawah kendali Satuan Kriminal Khusus. Di Poltabes/Polres lain yang menjadi sampling penelitian tidak ditemukan satuan/unit cyber crime, artinya secara kelembagaan organisasinya belum terbentuk. Berdasarkan data tersebut maka dapat dikatakan struktur organisasi unit cyber crime tingkat Polres masih lemah.

Hal di atas terjadi karena SOTK tingkat Polres kedudukan organisasinya mengikuti amanat Perkap No. 23 tahun 2010. Dalam perkap tersebut Kasat Reskrim membawahi 5 (lima) Kepala Unit, yaitu TP Umum, TP Korupsi, TP Khusus, PPA, dan Opsnal. Jadi belum terbentuk unit cyber crime di tingkat Polres, namun saat ini tugas pokok dan fungsi cyber crime masih diemban oleh Satuan Kriminal Umum, dan tidak jarang juga ditangani oleh unit TP Khusus. Oleh karena itu penanganan kasus-kasus/perkara cyber crime tidak dapat maksimal dan belum bisa memenuhi tuntutan pelayanan publik.

Sebagai gambaran berikut ini disampaikan hasil temuan lapangan tugas dan fungsi Satuan Reserse Kriminal Umum yang sekaligus secara ekplisit menggambarkan tugas bidang *cyber crime*. Satreskrim Polrestro/tabes dikepalai oleh seorang Pamen berpangkat AKBP, untuk tipe Polres dikepalai oleh seorang Pama berpangkat AKP.

Adapun tugas dan fungsinya sebagai berikut :

1. Urusan pembinaan operasional (Urbinopsnal), yang bertugas melakukan pembinaan dan pengawasan terhadap administrasi serta pelaksanaan penyelidikan dan penyidikan, menganalisis penanganan kasus dan mengevaluasi efektivitas pelaksanaan tugas Satreskrim.
2. Urusan administrasi dan ketatausahaan (Urmintu) yang bertugas menyelenggarakan kegiatan administrasi dan ketatausahaan.
3. Urusan Identifikasi (urident) yang bertugas melakukan identifikasi dan laboratorium forensik lapangan dan pengidentifikasian untuk kepentingan penyidikan dan pelayanan umum.
4. Unit terdiri paling banyak 6 (enam) unit yang bertugas melakukan penyelidikan dan penyidikan tindak pidana umum, khusus dan tertentu di daerah hukum Polres serta memberikan pelayanan dan perlindungan khusus kepada remaja anak dan wanita baik sebagai pelaku maupun korban sesuai dengan ketentuan peraturan perundang-undangan.

C. Analisa Struktur Organisasi Cyber Tingkat Polda dan Polres

1. Struktur Organisasi *Cyber Crime* Tingkat Polda

   Berdasarkan hasil penelitian lapangan di empat Polda yang menjadi sampling kajian diperoleh gambaran bahwa struktur organisasi *cyber crime* di tingkat Polda belum ada kesamaan. Polda yang memiliki struktur organisasi relative sama, yakni Polda Metro Jaya dan Polda Jawa Timur. Polda Jawa Barat walaupun Tipe A kedudukan organisasi *cyber crime* belum berdiri sendiri menjadi Subdit *cyber crime*, masih tergabung organisasinya dengan salah satu unit di subdit dirkrimsus, statusnya masih pada level Unit *cyber crime* belum berbentuk Subdit *Cyber.*

Di Polda Banten kedudukan organisasi *cyber crime* sama dengan di Polda Jabar masih level Unit *cyber crime* dibawah kendali salah satu Subdit Perbankan Direktorat Kriminal Khusus. Kedudukan struktur organisasi *cyber crime* sebagaimana yang ditemukan di Polda Jabar dan Banten tersebut tidak konsisten dengan kebijakan Kapolri dan tidak responsive terhadap permasalahan serta tantangan tugas bidang *cyber crime* yang sangat cepat tingkat eskalasinya. Dalam arti kedudukan organisasi *cyber* setingkat Unit di wilayah Polda kurang memadai dan tidak akan mampu mengoptimalkan kinerja bidang penegakan hukum *cyber crime.*

Sebab tugas dan tanggungjawab utama satuan organisasi *cyber crime,* yaitu

a. Penyidikan kasus-kasus yang berhubungan dengan transaksi elektronik, *money loundring*, pasar modal, pajak, perbankan, dll).
b. Penyidikan kasus-kasus yang berhubungan dengan teknologi komunikasi dan informasi (penyadapan telepon, penyalahgunaan Voip, penipuan melalui telepon genggam).
c. Penyelidikan kejahatan yang menggunakan fasilitas Internet (*cyber gambling, cyber terrorism, cyber fraud, cyber sex, cyber narcotism, cyber smuggling, cyber attacks on critical infrastructure, cyber black mail, cyber theatening*, pencurian data, pencemaran nama baik, dll)
d. Penyidikan kejahatan computer (masuk ke system secara illegal, *ddos atack, hacking, tracking, phreacing*, membuat dan menyebarkan yang bersifat merusak seperti *malicous code al viruses, worm, rabbits trojan*, dll).
e. Penyidikan kejahatan yang berhubungan dengan Hak atas Intelektual (Pirated Software, rekaman suara, merubah tampilan website)

Selain itu, penanganan tindak pidana *cyber* memerlukan (9) sembilan jenis kegiatan, yaitu:

a. Penyelidikan;
b. Penyidikan;
c. *Forensik digital* (pengolahan dokumen elektronik);

d. Perencanaan dan anggaran;
e. Pemeliharaan peralatan khusus;
f. Kerjasama;
g. Peningkatan kemampuan;
h. Unit taktis;
i. Akreditasi;

Berdasarkan temuan dalam penelitian lapangan, dari 9 (sembilan) kegiatan tersebut, saat ini hanya 3 (tiga) kegiatan yang terakomodir dalam struktur organisasi dan tata kerja Subdit IV *Cyber Crime* Dit Krimsus Polda Metro Jaya. Ketiga kegiatan tersebut adalah: penyelidikan, penyidikan dan forensik digital. Mengapa hal itu terjadi ? salah satu penyebabnya adalah cakupan kewenangan Subdit *Cyber* terbatas, apalagi bila berbentuk Unit dibawah Subdit akan jauh terbatas tingkat kewenangannya.

Oleh karena itu di tingkat wilayah Polda seyogyanya minimal berbentuk satuan organisasi Subdit *Cyber Crime,* sedangkan di wilayah Polda Metro Jaya perlu adanya peningkatan level organisasi menjadi Direktorat. Apabila struktur organisasi *cyber* berbentuk Direktorat *Cyber Crime* maka diharapkan 9 (Sembilan) jenis kegiatan bidang *cyber crime* dapat terlaksana dengan baik, karena secara empirik struktur organisasi Subdit hanya mampu melaksanakan 3 (tiga) jenis kegiatan yang berkaitan dengan tindak pidana digital/*cyber crime.*

Berangkat dari empat polda yang menjadi kajian atau sampling penelitian, maka yang perlu ditingkatkan statusnya menjadi Direktorat *Cyber Crime* adalah Polda Metro Jaya dan Polda Jawa Timur, sebab keduanya telah memiliki peralatan yang memadai dalam bidang *cyber crime,* seperti CCISO, laboratorium forensic, dan fasilitas lain. Kedudukan organisasi *cyber crime di* wilayah Polda Jabar dan Polda Banten juga perlu ditingkatkan levelnya menjadi Subdit *Cyber Crime* agar memiliki kewenangan lebih besar dan mampu mengantisipasi tuntutan tugas dalam bidang kejahatan siber yang semakin hari semakin meningkat, baik berkaitan dengan "*computer crime, computer reated crime maupun cyber fraud and phising"*.

Penanganan kejahatan siber di tingkat wilayah Polda juga menghadapi kendala yang berkaitan dengan tingkat efektivitas kinerja organisasi bidang *cyber crime* terutama berkenaan dengan SOP, Anggaran, laboratorium dan peralatan digital forensik, pemeliharaan dan perawatan. Gambaran yang berkenaan dengan analisis efektivitas organisasi cyber crime sebagai berikut

a. Standar Operasional Prosedur (SOP)
    1) Kinerja organisasi cyber tingkat Polda belum optimal karena regulasi yang berkenaan dengan penanganan kasus cyber crime belum diatur secara khusus, seperti :Kegiatan yang berkaitan dengan penyelidikan dan penyidikan kasus *cyber*
        a) Kegiatan atau aktivitas *cyber* patrol atau sosial media monitoring center
        b) Mekanisme tentang aksesibilitas data eksternal antara Mabes, Polda dan Polres
        c) Tenggang waktu Penghapusan data (Retensi data)
        d) Pertukaran data antar Negara (Reciprocall Data Digital)
        e) Pengelolaan data digital, pemeriksaan barang bukti digital oleh Pusiknas/DivTI
    2) Aturan yang berkenaan dengan penanganan kasus cyber crime yang sudah ada/terdukung, seperti :
        a) SOP tentang penggunaan alat khusus *Direction Finder*
        b) SOP tentang Laboratorium *Digital Forensik*

b. Anggaran
    1) Anggaran lidik sidik masih mengacu pada indeks Perkap 378 Tahun 2009 tentang anggaran lidik sidik kasus-kasus kriminal umum dengan ketentuan :
        a) indeks Mudah Rp. 4,740,000,-/kasus
        b) indeks Sedang Rp. 9,300,000,-/kasus
        c) indeks Sulit Rp. 14,925,000,-/kasus

d) indeks sangat sulit Rp. 24.900.000,-/kasus

2) Anggaran khusus operasionalisasi *Direction Finder,* tim analis dan petugas *cyber patrol* belum ada ketentuan indeks khusus

3) Anggaran khusus sertifikasi internasional para penyidik *cyber* 30 juta/orang yang harus di upgrade kemampuannya setiap 2 tahun sekali juga belum ada alokasi anggarannya

c. Laboratorium *Cyber*

1) Laboratorium *cyber crime* di tingkat Polda yang memiliki *Cyber Crime Investigation Satelit Office* (CCISO) baru Polda Metro Jaya dan Polda Jawa Timur.

2) Laboratorium *Strategic Informasi and Tactical Operation Centre* (SITOC) yang memiliki hanya Polda Metro Jaya, sedangkan ketiga Polda yang laian belum mempunyai.

d. Pemeliharaan dan Perawatan

Untuk kebutuhan anggaran pemeliharaan dan perawatan peralatan laboratorium *cyber* belum terdukung oleh DIPA Polri, sehingga menjadoi beban anggaran satuan organisasi *cyber crime* tingkat polda masing-masing.

Disamping itu persoalan beban tugas Subdit *Cyber* juga menjadi kendala karena pada umumnya sangat tidak sebanding antara jumlah kasus dengan kekuatan SDM yang dibutuhkan, hanya ± 30% kekuatan personel *cyber crime.* Kendala lain tidak hanya masalah kekuatan SDM dan tetapi juga kemampuan personil dan penyidik *cyber crime*, karena penyelidikan dan penyidikan bidang *cyber* menuntut persyaratan khusus, yaitu :

1) Kemampuan Bahasa Inggris

2) Kemampuan Komputer Forensik

3) Kemampuan Mobile Forensik

4) Kemampuan Analisis jaringan transaksi keuangan dan komunikasi

5) Kemampuan *cyber law*

Lima kemampuan pokok inilah yang sangat dibutuhkan untuk dapat mengembangkan kemampuan penyidik cyber, yang kini di lingkungan Polri juga masih sangat langka dan jarang ditemukan di tingkat wilayah Polda. Apabila persyaratan kemampuan tersebut terpenuhi maka penyidik *cyber* akan mudah memperoleh sertifikat internasional dalam bidang *cyber crime*. Jumlah penyidik *cyber crime* di Polda Metro Jaya yang memiliki sertifikat internasional baru 4 orang dari 7 orang penyidik, mereka memiliki sertifikasi program *Certified Ethical Hacker (CEH)* dan sertifikasi program *Computer Hacking Forensic Investigator Certification* (CHFI). Sementara Polda lain yang memiliki penyidik bersertifikat internasional yakni Polda Jawa Timur, Polda Banten dan Polda Jawa Barat belum memiliki penyidik yang bersertifikat CEH dan CHFI.

Selain hal tersebut di atas dari penelitian juga diperoleh infomasi dan data yang berkaitan dengan KIS (koordinasi, integrasi, singkronisasi) dan HTCK dalam melaksanakan tugas bidang *cyber crime*. KIS dan HTCK belum optimal dan MoU dengan pihak lembaga/instansi eksternal masih terbatas sehingga personel/penyidik siber lebih mengandalkan hubungan personal dalam memperoleh akses informasi tertentu. Persoalan ini menjadi kendala di tingkat lapangan terutama dalam penyelidikan dan penyidikan yang ingin diselesaikan dengan cepat karena kendala birokrasi di masing-masing instansi/lembaga tersebut.

2. Analisa Organisasi Cyber Crime di Tingkat Polres

a. Struktur Organisasi

Gambar 12. Struktur Organisasi Sat Reskrim Polres

Berdasarkan struktur tersebut di atas diperoleh gambaran bahwa struktur organisasi *cyber crime* di tingkat Polres tidak ada, dalam arti yang berwenang menangani bidang *cyber crime* atau kanit *cyber crime* belum ada.

Kedudukan struktur organisasi di tingkat Polrestro/Polres hingga kini masih berdasarkan Perkap Nomor 23 Tahun 2010. Berdasarkan perkap tersebut Kasat Reskrim mengendalikan 5 (lima) Unit, yaitu Kanit TP Umum, Kanit TP Korupsi, Kanit TP Khusus, Kanit PPA dan Kanit Opsnal. Dengan demikian kedudukan organisasi *cyber crime* di tingkat Polres dapat diambil simpulan bahwa :

1) Struktur organisasi *cyber crime* di tingkat Polres belum ada, saat ini tugas pokok dan fungsi dengan tugas rangkap oleh Satkrimum, sehingga penanganan kasus/perkara cyber tidak maksimal dan belum bisa memenuhi efektasi masyarakat.
2) untuk Satreskrim Polrestro/tabes dikepalai oleh seorang Pamen berpangkat AKBP, untuk tipe Polres dikepalai oleh seorang Pama berpangkat AKP.
3) Kasatreskrim Polres membawahi (Urident, Urmintu, Urbinops) dan membawahi 5 Unit serta mayoritas jajaran Polres Metro secara struktural belum terbentuk kecuali di Polres Metro Jakarta Barat dengan memiliki unit cyber tersendiri dan langsung dipimpin oleh Kasat.

Pada umumnya tingkat Polres kasus-kasus yang berhubungan dengan kejahatan siber ditangani oleh Tindak Pidana Umum atau Tindak Pidana Khusus dan tertentu, sesuai dengan substansi kasusnya. Artinya, walaupun belum ada secara organisatoris struktur organisasi *cyber crime* tingkat Polres namun dalam penegakan hukum siber dilaksanakan oleh Unit Tindak Pidana Umum atau dan Tindak Pidana Khusus dan tertentu.

Lemahnya struktur organisasi *cyber crime* tingkat Polres inilah yang menjadi kendala utama penegakan hukum siber *(cyber law)* pada tingkat wilayah hukum Polres. Pada hal garda utama pelayanan publik, pengayoman, dan perlindungan serta penegakan hukum sebenarnya adalah di tingkat Polres.

Selain itu dampak Perkap 23 Tahun 2010 di tingkat Polres, yaitu pertama, struktur organisasi *cyber crime* di tingkat polres tidak ada, kedua, pelayanan di bidang penegakan hukum siber relative lemah karena tidak ada unit yang secara mandiri mengemban tugas pokok fungsi bidang kejahatan siber. Sedangkan kondisi empirik, menunjukkan trend kejahatan *cyber* terus meningkat dari tahun ke tahun, mulai dari penipuan *on line, skiming* dan *phising* ATM, narkoba, ujaran kebencian, hoax, dan sebagainya.

Laporan masyarakat yang berkaitan dengan kejahatan semakin banyak dan tidak mudah penyelidikan dan penyidikannya. Persoalan ini belum dikaitkan dengan pola pelayanan polri yang menitrikberatkan pada kekuatan utama pelayanan pada tingkat Polres.

Kondisi struktur organisasi Polres yang belum menempatkan unit/satuan *cyber crime* semacam itu dalam perspektif kelembagaan disebut miskin struktur, pada hal kegiatannya atau tugas pokoknya sudah dilaksanakan selama ini. Dalam konteks inilah diperlukan pengembangan atau penataan organisasi di tingkat Polres terutama yang menangani urusan *cyber crime.* Sebab tugas/kegiatanya sudah dilaksanakan tetapi organisasinya belum ada.

Pengembangan atau penambahan struktur organisasi dalam kajian teoritik memang dibenarkan apabila suatu beban kerja bertambah berat, dan pekerjaan tertentu sudah dilaksanakan tetapi masih dirangkap oleh unit organisasi lain. Kondisi semacam itu akan

mempengaruhi kinerja dalam bidang *cyber crime*. Oleh karena itu penyelesaian dan penegakan hukum di bidang *cyber crime* tingkat Polres tidaklah dapat optimal karena salah satu kendalanya faktor kedudukan dan kemampuan organisasi tingkat Polres masih lemah.

Dengan kata lain, masalah *cyber crime* di tingkat Polres belum dijadikan focus dalam penegakan hukum, sementara laporan masyarakat yang berkaitan dengan kejahatan siber semakin meningkat. Hasil kajian lapangan dari forum group diskusi dengan para Kapolres, Kapolsek, Kasat, Kanit dan anggota personel reskrim diperoleh informasi dan data bahwa kasus-kasus *cyber crime* dari hari kehari semakin meningkat, baik yang berkaitan dengan penipuan on line, pencurian ATM, penghinaan dan fitnah melalui medsos, ujar kebencian, dll.

Sementara kemampuan Polres sekarang dihadapkan dengan realita struktur organisasi dan tuntutan pelayanan masyarakat, karena itu harus ada satuan organisasi yang secara khusus menangani masalah kejahatan *cyber crime.*

Berangkat dari hasil penelitian di berbagai Polres sampling diperoleh simpulan, bahwa satuan organisasi *cyber crime* sangat dibutuhkan agar persoalan yang berkaitan dengan kejahatan siber dapat diselesaikan secara maksimal. Polres kini membutuhkan penguatan struktur organisasi agar lebih responsive dalam menjalankan tugas penegakan hukum, karena pola kejahatan telah bergeser dari konvensional ke arah modern dan digital. Struktur organisasi *cyber crime* di tingkat Polresta/tabes lebih tepat berbentuk Satuan tersendiri (*Satuan Cyber Crime*), sedangkan di tingkat Polres lainnya berbentuk *Unit Cyber Crime*.

b. Kemampuan Sumberdaya Organisasi

Dalam menangani kasus-kasus tersebut Polres masih menghadapi kendala baik yang berkaitan dengan struktur organisasi

maupun kemampuan sumberdaya organisasi. Dampak kondisi semacam itu maka Polres cenderung bersikap ‘menerima laporan’ dari pengaduan masyarakat, apabila kasusnya besar berkaitan dengan pejabat publik dan nilai kerugiannya besar maka dialihkan/disarankan pengaduannya ke tingkat Polda dengan alasan hal itu menjadi kewenangan tingkat Polda.

Sedangkan di sisi lain kemampuan sumberdaya organisasi Polres masih terbatas, sebagai misal jumlah DSP dan realita belum memenuhi rasio ideal. Jumlah personel reskrim belum sebagaimana yang diharapkan sehingga banyak kasus yang belum terselesaikan dan keterbatasan jumlah penyidik yang memenuhi syarat peraturan perundang-undangan hukum pidana. Ditingkat Polres juga belum ada tim analis, tim direction finder, tim digital forensik.

Kendala yang dihadapi Polres kini sebenarnya berkaitan dengan bergesernya kejahatan dari konvensional ke digital atau elektronik, sifat kejahatan transnasional dan internasional itu kejahatannya bersifat *cyber* (maya) sehingga tidak dapat dibuktikan tanpa menggunakan pendekatan ilmiah dan digital forensik. TKP nya belum tentu di suatu tempat tetapi bisa di berbagai tempat, sedangkan kemampuan personel Polres dalam bidang *cyber crime* sangat terbatas.

Personel penyidik dan lidik yang menangani kasus *cyber* belajar mandiri dengan biaya sendiri karena selama ini belum ada dikjur *cyber crime.* Sehingga hak itu berpengaruh terhadap penyelesaian kasus *cyber crime*, rata-rata kasus tersebut baru sampai tahap lidik dan belum ada tindak lanjut karena terbentur sarana dan prasarana serta peralatan. Jumlah kasus yang sampai P21 sangat kecil di tingkat Polres.

c. Laboratorium dan Peralatan

Selain itu sumberdaya persoalan yang berkaitan dengan peralatan/ laboratorium *digital forensic* di tingkat polres belum ada sehingga dalam penanganan kasus harus meminjam peralatan dari Polda. Ditingkat Polres belum tergelar peralatan TI maupun Laboratorium mini cyber yang dapat dipergunakan untuk mendukung pengungkapan kasus *cyber crime* (seperti *Direction Finder, Cellebrite, Call Data Record, check pos,* dll) bahkan komputer pun sebagai kelengkapan perorangan masih menggunakan komputer pribadi masing-masing penyidik.

d. Efektivitas Kinerja Satuan Cyber Crime

Kendala lain yang muncul berkaitan dengan penanganan dan penegakan *cyber crime* di tingkat Polres adalah berkenaan dengan tingkat efektivitas kinerja satuan *cyber crime*, yaitu :

1) Standar Operasional Prosedur

Kinerja organisasi *cyber* tingkat Polres belum berjalan secara optimal karena regulasi yang berkenaan dengan penanganan kasus *cyber crime* belum ada, saat ini Satreskrim Polres dalam penanganan kejahatan kasus *cyber* hanya mengacu pada Perkap penyelidikan dan penyidikan umum, komposisi pembagian tugas serta pembidangan kompetensi personel pun juga belum jelas, sehingga terjadi ambigu dikalangan penyidik.

2) Penyelidikan terhadap pelaku tindak pidana *cyber* terhalang Undang-Undang atau regulasi yang mengikat dimasing-masing sektor, dimana data pelaku tidak bisa diperoleh/diakses dari pihak eksternal (Bank, provider, Dukcapil, dll) sebelum dibangun “MOU” secara bersama.

3) Anggaran

Anggaran lidik sidik *cyber* masih menggunakan acuan Perkap 14 Tahun 2012 tentang manajemen penyidikan kasus-kasus kriminal umum dengan kriteria :

a) indeks Mudah Rp. 4,740,000,-

b) indeks Sedang Rp. 9,300,000,-

c) indeks Sulit Rp. 14,925,000,-

4) Laboratorium dan peralatan *cyber crime*

Laboratorium digital forensic di tingkat Polres belum ada sehingga dalam penanganan kasus harus meminjam peralatan dari Polda. Ditingkat Polres belum tergelar peralatan TI maupun Laboratorium mini *cyber* yang dapat dipergunakan untuk mendukung pengungkapan kasus *cyber crime* (seperti *Direction Finder, Cellebrite, Call Data Record, check pos,* dll)

5) Pemeliharaan dan Perawatan

Anggaran pemeliharaan dan perawatan peralatan laboratorium di tingkat Polres belum terdukung oleh DIPA Polri sebab belum memiliki peralatan/Laboratorium *cyber.*

Berdasarkan wawancara dan hasil forum group diskusi dengan para pejabat fungsi di tingkat polres dan polsek diperoleh data dan informasi, sebagai berikut :

a. Kendala yang dihadapi oleh Polres dalam menangani kasus *cyber crime* karena belum terbangun aturan hubungan tata cara kerja yang memberikan *"aksesibility"* dan wewenang tingkat Polres mengakses data/informasi kepada pihak eksternal (provider, bank, dll) akses untuk mengungkap masalah harus melalui birokrasi Polda sehingga tidak bisa cepat.
b. HTCK masih bersifat birokratis belum responsif terhadap kecepatan dalam melaksanakan tugas sehari-hari. HTCK Polres – Polda yang terbangun bersifat hubungan personal bukan institusi, sehingga birokrasi untuk meminjam peralatan direction finder harus antri dan sering terkendala.
c. Kordinasi integrasi dan sinkronisasi antara Polres dan Polda serta pihak eksternal belum optimal karena tidak ada "MOU" dengan *stakeholders* untuk masalah *cyber crime.*

d. Hubungan dalam aksesbilitas data eksternal untuk mendukung pengungkapan kasus *cyber* yang terjadi masih mengedepankan hubungan emosional pendekatan personal (pertemanan) daripada institusional.

BAB V
KESIMPULAN DAN REKOMENDASI

A. Kesimpulan

1. Satuan Fungsi *Cyber* Tingkat Polda

a. Struktur organisasi *cyber crime* tingkat polda saat ini masih dibawah kendali Direktorat Krimsus Polda, kedudukan organisasinya sebagai salah satu Subdit di Direktorat Kriminal Khsusus. Subdit *Cyber Crime* dipimpin oleh Kasubdit dengan pangkat AKBP. Jumlah personel subdit *cyber crime* relative kurang karena kekuatan personel hanya sekitar 30 % dari DSP yang dibutuhkan.

b. Kemampuan dan kualitas penyidik *cyber crime* kebanyakan belum bersertifikat nasional ataupun internasional. Kecuali di Polda Metro Jaya 4 (empat) personel sudah berkualifikasi standar internasional. Di Polda Jatim setidaknya ada dua personel *cyber crime* yang sudah bertaraf internasional walaupun belum memiliki sertifikasi internasional (kualifikasi CEH maupun CHFI). Di Polda Jabar dan Polda Banten belum mempunyai personel yang bersertifikat internasional, tetapi beberapa personel memiliki kemampuan dalam bidang IT, computer dan komunikasi.

c. Anggaran untuk penanganan kasus kejahatan *cyber crime* belum ada perkapnya, sehingga tidak ada acuan khusus untuk anggaran lidik sidik *cyber crime*. Anggaran lidik sidik masih mengacu pada anggaran pidana umum pada hal proses lidik dan sidik kejahatan siber jauh berbeda dengan kejahatan konvensional. Lidik dan sidik *cyber crime* syarat dengan teknologi IT, sistem informasi, dan analisis digital forensic yang memerlukan biaya cukup tinggi.

d. Sarana prasarana serta peralatan untuk menangani kejahatan *cyber crime* tingkat Polda relative beragam, baik gedung, laboratorium,

maupun peralatan utama *cyber crime.* Misalnya, DF, CDR, Cellebrite, CCISO SITOC dan lain-lain. Polda yang memiliki CCISO dan SITOC baru Polda Metro Jaya, Polda Jatim sudah memiliki CCISO tetapi SITOC belum memiliki. Polda Jabar dan Banten CCISO belum memiliki. Mobile DF yang memiliki baru Polda Metro Jaya dan Polda Jatim, sedangkan Polda Jabar dan Polda Banten belum memiliki mobile DF.

2. Satuan Fungsi *Cyber* Tingkat Polres

a. Struktur Organisasi satuan *cyber* ditingkat Polres belum terbentuk, kasus kejahatan *cyber* yang dilaporkan masyarakat terus meningkat per hari 1 – 5 kasus, dan perkaranya saat ini ditangani oleh Satreskrimum.

b. Kemampuan Sumberdaya personel masih terbatas, baik dari segi kualifikasi penyidik *cyber* maupun kuantitas personel. Di tingkat polres penyidik yang menangani kejahatan *cyber* belum memiliki kemampuan atau keahlian penyidik *cyber crime,* artinya belum ada yang memiliki sertifkat diklat *cyber.* Personel yang mengemban tugas lidik dan sidik *cyber crime* masih merangkap tugas pada fungsi kriminal umum. Kemampuan anggaran dalam lidik dan sidik *cyber* masih bertumpu pada anggaran criminal umum. Kemampuan peralatan, Polres belum memiliki peralatan untuk mengungkap kasus kejahatan cyber, seperti. laboratorium mini *digital forensic, cellebrite, check post,* dan lain-lain sebagai sarana utama dalam mengungkap kejahatan *cyber,* saat ini apabila menangani kasus masih meminjam alsus ke Polda.

B. Rekomendasi

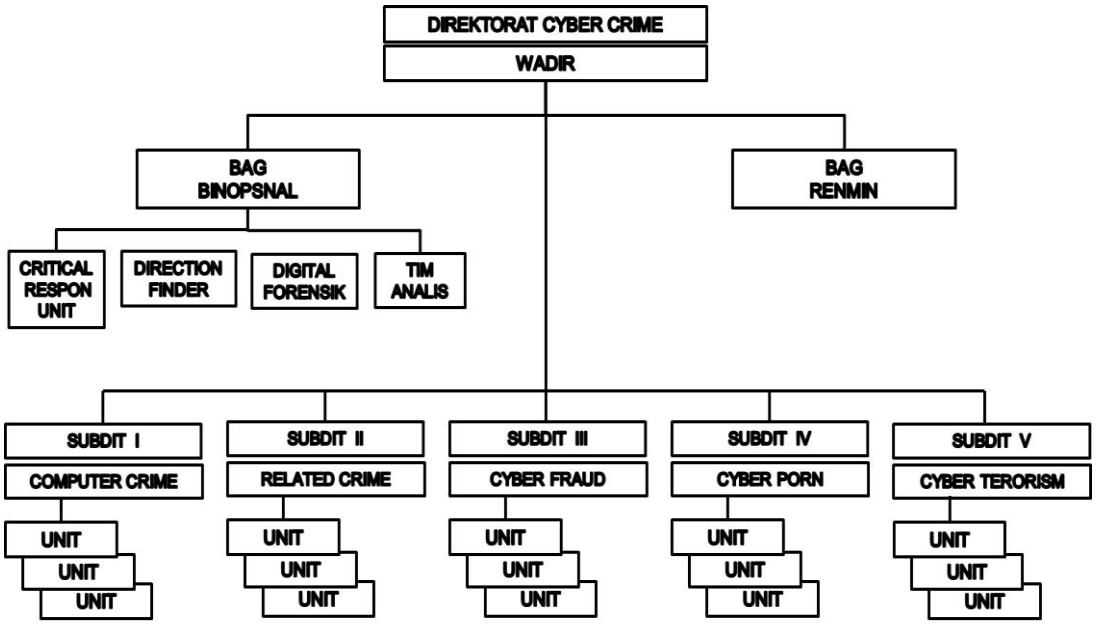
1. Satuan Fungsi Cyber Tingkat Polda

a. Struktur organisasi *cyber crime* tingkat Polda khsususnya Polda tipe A perlu dibentuk Direktorat *Cyber* Polda, sedangkan polda Tipe B dalam bentuk Direktorat tetapi skeleton.

b. Personel yang mengemban tugas lidik dan sidik bidang *cyber crime* perlu segera diikutkan diklat/dikjur *cyber crime.*

c. Anggaran lidik dan sidik bidang *cyber crime* perlu dibedakan dengan anggaran dengan lidik dan sidik kriminal umum sebab penegakan hukum *cyber crime* syarat dengan peralatan teknologi dan informasi digital.

Adapun rekomenadsi desain struktur organisasi *Cyber Crime* tingkat Polda (Tipe A) sebagai berikut :



2. Satuan Fungsi *Cyber* Tingkat Polresta/bes dan Polres

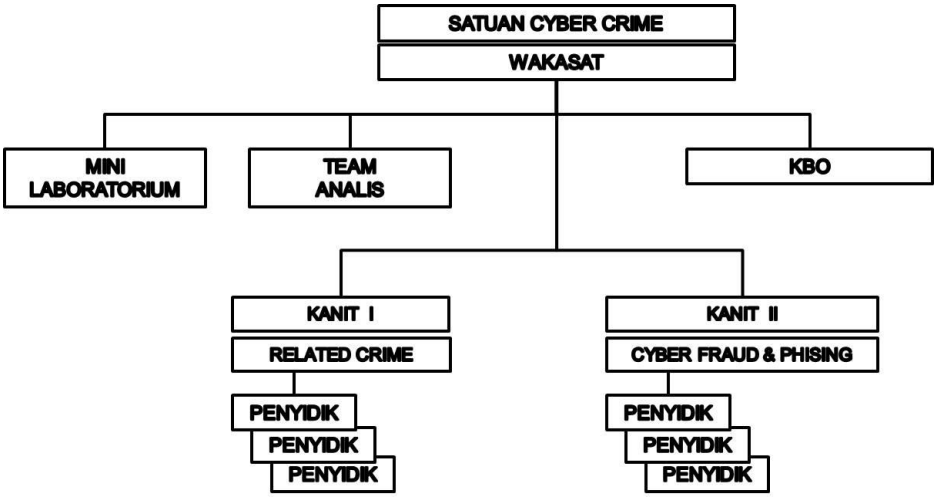
1. Struktur Organisasi

   Dalam rangka merespon besarnya tuntutan masyarakat dan semakin meningkatnya kejahatan *cyber,* di tingkat jajaran Polresta/bes perlu dibentuk Satuan *Cyber Crime* namun untuk tingkat Polres bentuk yang lebih responsive Unit *Cyber Crime,* karena berhubungan dengan sumberdaya organisasi polres. Apabila Satuan *Cyber Crime* dibentuk maka strukturnya dalam bentuk skelton.

2. Personel yang mengemban tugas lidik dan sidik bidang *cyber crime* perlu segera diikutkan diklat/dikjur *cyber crime* dan diagendakan dalam kalender akademik Lemdiklat Polri

3. Anggaran lidik dan sidik bidang *cyber crime* perlu dibedakan dengan anggaran dengan lidik dan sidik kriminal umum sebab penegakan hukum *cyber crime* syarat dengan peralatan teknologi dan informasi digital.

Adapun rekomendasi desain struktur organisasi tingkat Polres sebagai berikut :



3. Nomenklatur nama Direktorat *Cyber crime* sebaiknya dirubah menjadi *Cyber Cop*

4. Perlu dioptimalkan dan di *upgrade* penggelaran peralatan dan SDM satuan *cyber crime* di Polda sampel secara terencana dan konsisten

BAB VI
PENUTUP

Demikian laporan akhir hasil kajian tentang **"Pengembangan Satuan Unit Cyber Crime di Tingkat Kewilayahan (Polda dan Polres)"** telah disusun. Semoga dapat dijadikan sebagai bahan masukan kepada Pimpinan Polri dalam menetapkan kebijakan lebih lanjut.

Bogor, Desember 2018

KETUA POKJA

Drs. M. ASRUL AZIZ, M.AP
KOMBES POL NRP. 63100752

DAFTAR SUSUNAN TIM PENELITI :

1. KBP. Drs. SYAMSUDIN DJANIEB, MM ……
2. PROF. DR. BAMBANG WIDODO UMAR ……
3. DR. CHAIRIL NUR SIREGAR .....
4. DRS. PRIYO, H.AR, S.Sos, M.PA, Ph.D (condt) .....
5. AKBP. WADI, SH. MH ……
6. AKBP. RAHMAT SYUKRI ……
7. KOMPOL. GALIH INDRAGIRI, S.I.K ……
8. PENATA. FAJAR ISTIONO, S.T ……
9. PENDA. YULI PERTIWI, S.E, M.M ……
10. IPDA. GUSTIKA SITANGGANG ……
11. PENGATUR I. HERY SUYANTO ……..

DAFTAR PUSTAKA

Aryan, 2012. *http://cybercrimeeptik.blogspot.com/2012/11/karakteristik-cybercrime.html*

Hari Anto, 2012. *http://malingduniamaya.blogspot.com/2012/09/karakteristik-cybercrime.htm*

Muhammad Nuh Al Azhar, MSc, CHFI., CEI., ECIH. 2018. *Bank Frauds and Digital Forensic : From Digital Era and Case Studies to Digital Forensic and Cyber Law*. Jakarta: *Police Superintendent- Senior Digital Forensic Analyst*

Keputusan Kapolri. 2017. Keputusan Kepala Kepolisian Negara Republik Indonesia *Nomor:Kep/136/II/2017 tentang Pengesahan Nomenklatur dan Titelatur Eselon*

IIA Ke Atas Pada Susunan Organisasi Polri Tingkat Mabes Polri. Jakarta: Kepala Kepolisian Negara Republik Indonesia.

Peraturan Presiden. 2017. Peraturan Presiden Nomor 5 Tahun 2017 *tentang Perubahan atas Peraturan Presiden Nomor 52 Tahun 2010 tentang Susunan Organisasi dan Tata Kerja Kepolisian Negara Republik Indonesia.* Jakarta: Presiden Republik Indonesia

Peraturan Kapolri. 2010. Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 21 Tahun 2010 *tentang Susunan Organisasi Dan Tata Kerja Tingkat Mabes Polri.* Jakarta

Priskanta Tarigan. 2011. *http:// freezcha.wordpress.com /2011/02/28/ penanggulangan-cybercrime/*

Undang-Undang. 2008. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 *tentang informasi serta transaksi elektronik, atau teknologi informasi secara umum.* Jakarta

Undang-Undang. 2008. Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang Hukum Acara Pidana. Jakarta

Undang-undang. 1999. Undang-Undang Republik Indonesia Nomor 36 tahun 1999 tentang Telekomunikasi.

Wibowo Tunardy, 2009 *http://www.wibowotunardy.com/pengertian-cybercrime/*