BAB II

KEJAHATAN DUNIA MAYA DI INDONESIA

Cyber crime merupakan kejahatan yang menggunakan teknologi informasi dan komunikasi dengan menggunakan computer, zaman global yang sedang berlangsung seperti saat ini mengubah kehidupan manusia baik secara komunikasi dan mnunjang pekerjaan tidak bisa lepas dari peranan teknologi informasi dan komunikasi. Dalam hal ini, sebagai contoh dengan maraknya penggunaan komputer yang menawarkan berbagai macam program aplikasi untuk menunjang efesiensi pekerjaan kita hingga merambat ke alat komunikasi yang juga menawarkan berbagai macam fasilitas dan program penunjang lainnya.

Dari perkembangan itu juga memberikan kesempatan pada segelintir orang yang tidak bertanggung jawab untuk memanfaatkanya sebagai sarana aksi kejahatan yang dapat merugikan orang lain. dari fenomena tersebut maka dapat diartikan bahwa kejahatan konvensional beralih ke kejahatan virtual *(cyber*), walau dilakukan dengan cara virtual namun memiliki dampak yang nyata *(real*). Hal inilah yang menyebabkan para pengguana teknologi menjadi lebih waspada.

Pada bab ini akan dijelaskan berbagai macam kejahatan *cyber* dari awal mula perkembanganya hingga berbagai jenis dan modus yang digunakan dengan menggunakan teknologi sebagai sarana kejahatan untuk meraup keuntungan yang merugikan pengguna teknologi informasi. Dari berbagai macam hasil penelitian dan survey juga menujukan bahwa tingkat serangan *cyber crime* dari tahun ke tahun semakin lama semakin meningkat termasuk di Indonesia, dengan fakta tersebut maka sudah dapat dipastikan penggunaan teknologi informasi juga masih di bilang belum aman oleh pengguna jasa teknologi informasi baik oleh warga Indoensia dan masyarakat dunia.

A. Kejahatan *Cyber Crime*

Berbicara masalah *cyber crime* tidak lepas dari permasalahan keamanan jaringan komputer atau keamanan *internet* dalam era global ini., apalagi jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan

pelayanan agar apa yang disajikan tidak mengecewakan pelangganya. Untuk mencapai tingkat kehandalam tentunya informasi itu sendiri harus selalu dimukhtahirkan sehingga informasi yang disajikan tidak ketinggalan zaman. Kejahatan dunia maya *(cyber crime)* ini muncul seiring dengan perkembvangan teknologi informasi yang begitu cepat untuk lebih mendalam ada beberapa pendapat dibawah ini tentang apa yang dimaksud dengan *cyber crime*? Diantaranya adalah menurut kepolisisan Inggris, *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal/atau kriminal berteknologi tinggi dengan mneyalah gunakan kemudahan teknologi digital.[1] Sedangkan menurut Peter, *Cyber crime* adalah

" The easy of cyber crime is crimes directed at computer or a computer system. The nature of cyber crime, however, is more complex. As we will see later, cyber rime can take the form of simple snooping into a computer system for which we have no authorization it can be the feeing of computer virus into the wild. It may be malicious vandalism by a disgruntled employee. Or it may be theft of data, money, or sensitive information using a computer system. [2]

Indra Safitri mengemukakan bahwa kejahatan dunia maya jenis kejahatan yang memanfaatkan sebuah teknologi informasi tanpa batas serta memiliki karakterisktik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan pada tingkat keamanan yang tinggi dan kredibilitas sebuah informasi yang disampaikan dan diakses oleh pelanggan *internet.*[3] Dalam dua dokumen kongres PBB yang dikutip oleh Barda Nawawi Arief, mengenai *The Prevention Of Crime And Treatment Of Offenders* di Havana kuba pada tahun 1990 dan di Wina Austria pada tahun 2000, menjelaskan ada dua istilah yang terkait dengan *cyber crime* yaitu *cyber crime* dan *computer related crime.* [4] Dilihat dari berbagai definisi di atas, tampak bahwa bekum ada kesepakatan mengenai definisi tentang *cyber crime* atau kejahatan dunia *cyber*.

---

[1] Abdul Wahid dan Mohammad Labib*, Kejahatan Mayantara (Cyber Crime*), Jakarta: PT. Rafika Aditama, 2005), hal. 40

[2] Peter Stephenson, *Investigating Computer Related Crime* : A Handbook for Cooperate Investigators, (London New York Washington D.C :CRS Press,2000), hal. 56

[3] Indra Safitri, *"Tindak Pidana Di Dunia Cyber "* dalam Insider, Legal Jurnal Forum Indonesia Capital & Invesment Market.

[4] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penagnggulangan Kejahata*n, (Jakarta, Kencana Perdana Media Group, 2007), hal 24

A. 1 Kejahatan dalam Pengertian Sosiologis

Pengertian kejahatan mengndung konotasi tertentu, dan merupakan penamaan yang bersifat relatif, menurut JE Sahetapy dan B Marjono Reksodiputro, pengertian kejahatan sebenarnya hanya merupakan suatu nama atau cap (label stigma) yang diberikan oleh orang-orang terntu untuk menilai perbuatan-perbuatan dari seseorang atau sekelompok orang sebagai perbuatan jahat. Pengertian kejahatan sangat dipengaruhi oleh nilai-nilai yang dianut oleh masyarakat.[5]

A. 2 Kejahatan Dalam Pengertian Yuridis

Kriteria kejahatan dalam arti yuridis pun dapat berubah dari waktu ke waktu. Istilah kejahatan adalah sebutan yang diberikan atau yang diletakan pada salah satu jenis atau yang diletakan pada salah satu jenis perbuatan manusia diantara perbuatan-perbuatan lainya. Perbuatan jahat dianggap melanggar atau bertentangan dengan apa yang ditentukan dalam kaidah peraturan perundang-undangan misalnya mencuri, membunuh atau tidak memenuhi panggilan pengadilan, dalam prespektif hukum kejahatan adalah segala perbuatan yang melanggar ketentuan hukum sebagaimana yang di atur dalam kitab KUHP maupun perundang-undangan tertulis lainya.

A. 3 Fenomena Kejahatan *Cyber Crime*

Revolusi Industri di Inggris pada abad ke 17 memacu perkembangan ilmu pengetahuan, teknologi, dan seni. Perkembangan tersebut berpengaruh pada kehidupan manusia. Terhitung sejak revolusi Industri, saat ini masyarakat telah memasuki siklus 50 tahunan yang ke lima, dengan ciri penggunaan Microelektronik dan Bioteknologi.[6] Senada dengan pernyataan tersebut Eddy Junaedy Karnasudirja mengungkapkan bahwa msayarakat saat ini sedang mengalami revolusi kedua, yaitu revolusi informatika yang ditandai dengan banyaknya penggunaan mesin sebagai pengganti fungsi otak manusia. Salah satu mesin tersebut adalah komputer.[7] Ari Juliano Gema mengemukakan bahwa kemajuan teknologi informatika dan komputer yang pesat melahirkan internet sebagai fenomena baru dalam kehidupan manusia. Selain itu Agus Rahardjo berpendapat internet merupakan sebagai jaringan komputer yang terhubung melalui media komunikasi, misalnya kabel telpon serat

[5] JE Sahetapy dan B Marjono Reksodiputro 1983
[6] Menuju teknologi berperikemanusiaan Jakarta 1996
[7] eddy junaedy karnasudirja bahaya kejahatan computer Jakarta 1999

optic, satelit atau gelombang frekuensi. Jaringan komputer tersebut terhubung antar Negara melalui *Transmission Protocol Control* (TPC) atau *Internet Protocol* (IP). Kehadiran internet memudahkan manusia untuk memperoleh informasi dan memudahkan menjalankan urusan urusanya di tingkat nasional maupun internasional misalnya dalam bidang pendidikan, kebudayaan, kekerabatan, teknologi, kesenian perdagangan, perbankan dan pemerintahan. Meskipun demikian internet dapat menimbulkan dampak negatif yang merugikan masyarakat misalnya pemalsuan, pencurian, penipuan, provokasi, pornografi, perjudian pembajakan hak cipta.

Pada awalnya komputer dikembangkan dari peralatan kalkulasi dalam bidang ilmu hitung. Dan saat ini menghasilkan pengelolaan sistem data yang tak terbatas. Sistem komputer juga mampu untuk mengendalikan sistem lalu lintas di darat, udara, dan laut. Sistem komputer bermanfaat dalam kegiatan perindustrian, perdagangan, dan perbankan. Meskipun demikian tidak dapat diabaikan bahwa ada beberapa orang menggunakan teknologi komputer untuk melakukan kejahatan misalnya *hecking* dengan alasan menyukai tantangan teknologi, spionase terhadap industri atau perusahaan orang lain, penipuan, gangguan sistem perdagangan lalu lintas sistem informasi.

A. 4 Sejarah Awal Terjadinya *Cyber Crime*

Penelitian tentang bentuk-bentuk *cyber crime* sudah dilakukan *Stenford Research International* (SRI) di Amerika serikat sejak 1971 sampai tahun 1985. Penelitian tersebut menemukan 1600 kasus yang terjadi sejak tahun 1958, serta reaksi masyarakat dan pemerintah terhadapnya, termasuk penyelesaian berdasarakan hukum perdata. Dalam tahun 1979 SRI mendapatkan data yang lebih valid, yaitu menyatakan bahwa dari 244 kasus yang terjadi, ada 191 yang dapat diajukan ke pengadilan dan terdakwa dari 161 kasus dapat dipidana. Penelitian- penelitian yang dilakukan pada tahun 1970-an tersebut belum dapat menunjukan data secara jelas pengaturanya dalam hukum pidana sehingga belum dimasukan ke dalam statistik kriminal.[8] penelitian lainya dilakukan di Jerman, Australia, Inggris, Swedia, Finlandia, Austria, Jepang, Kanada, Belanda. Semua penelitian tersebut bahwa *cyber crime* selalu meningkat dari tahun ke tahun.[9] Beberapa bentuk *cyber crime* di

[8] Eddy Junaedy Karnasudirja bahaya kejahatan computer Jakarta 1999
[9] Ibid p 20-22

amerika serikat yang menarik perhatian masyarakat antara tahun 1974 sampai tahun 1988 adalah sebagai berikut.

a. Tahun 1974

   Sejumlah mahasiswa Brooklyn Collage New York mengakses secara tidak sah pada data komputer ke bagian registrasi akademi, kemudian mengubah data pada daftar prestasi akademik milik mereka sendiri dan teman-temanya secara *online.* Setelah diadakan investigasi perbuatan tersebut terbukti diakukan oleh 12 mahasiswa[10]

b. Tahun 1977

   Dua orang karyawan bagian pemograman komputer dalam suatu perusahaan menggunakan komputer perusahaan tersebut secara tidak sah selama 3 tahun. komputer tersebut digunakan untuk memenuhi kebutuhan perusahaan lainya yang di dirikan oleh pelaku kejahatan. [11]

c. Tahun 1986

   Tiga orang anak ditahan oleh kepolisian amerika serikat karena diduga kuat menghancurkan sistem kemanan TRW perusahaan kartu kredit dan mengopy nomor kartu kredit orang lain kemudian membelanjakan USD 10.000.[12]

d. Tahun 1988

   Seorang mahasiswa berhasil memasukan *virus Internet-Worm* dalam sistem internet yang mengakibatkan ganggaguan terhadap 6000 sistem internet

Berdsarakan putusan pengadilan, *cyber crime* terjadi di Indonesia sejak tahun 1983, yaitu kasus pembobolan Bank Rakyat Indonesia (BRI) Cabang Brigjend Katamso Yogyakarta pada tahun 1986 terjadi pembobolan Bank Negara Indonesia (BNI 1946) dengan cara menggunakan fasilitas komputer. Pada tahun 1989 terjadi pembobolan bank Bali dengan tersangka Budiman Hidayat. Pada tahun 1990 terjadi *cyber crime* di bandung, yaitu pengopian secara tidak sah terhadap program *Word Star* versi 5.0[13] dalam tahun-tahun beikutnya Indonesia banyak terjadi *cyber crime* misalnya *cracking*, pemalsuan kartu kredit

[10] Aloysius Wisnubroto Yogyakarta 1999
[11] Ibid
[12] Suheimi 1990
[13] Aloysius Wisnubroto Yogyakarta 1999
[13]Sabartua Tampubolon 2001

(*carding*), pembobolan bank, pornografi, termasuk penyalahgunaan nama domain (*domain name*).[14]

A. 5 Laporan *Symantec Internet Security Threat Report*

Aktivitas kejahatan *cyber* di Indonesia meningkat tajam. Menurut perusahaan keamanan *Symantec* dalam *Internet Security Threat Report* volume 17, Indonesia menempati peringkat 10 sebagai negara dengan aktivitas kejahatan *cyber* terbanyak sepanjang tahun 2011. Indonesia menyumbang 2,4% kejahatan *cyber* di dunia. Angka ini naik 1,7% dibanding tahun 2010 lalu di mana Indonesia menempati peringkat 28.“Ini peningkatan yang sangat signifikan,” ujar *Senior Director Systems Engineering Symantec South Asia* Raymond Goh, dalam jumpa pers di Jakarta pada Selasa (15/5/2012). Hal ini tak lain disebabkan oleh terus meningkatnya jumlah pengguna internet di Indonesia.

Terlebih, Indonesia masuk lima besar pengguna jejaring sosial terbanyak di dunia. Menurut Raymond, penjahat *cyber* kini mulai melirik situs jejaring sosial untuk aksi kejahatan. Sifat “pertemanan” dalam jejaring sosial membuat pengguna percaya begitu saja atas *link* atau konten yang mereka terima dari sesama teman.“ Mereka tidak sadar bahwa *link* yang mereka terima mengandung program jahat, misalnya mereka dibawa ke situs web berbahaya,” tambah Raymond.Berdasarkan penelitian *Symantec*, Indonesia juga tercatat menempati peringkat 6 di dunia untuk kategori program jahat *spam zombie.*

Padahal pada 2010 lalu, Indonesia masih menempati peringkat 28 untuk *spam zombie.*Para penjahat yang menyebarkan *spam zombie* dapat mengendalikan sebuah nomor telepon seluler di *smartphone* untuk menyebarkan SMS premium, demi mendapatkan keuntungan finansial.Sementara untuk kasus pencurian data dan informasi, Indonesia bercokol di posisi 27 setelah tahun 2010 lalu menempati urutan 30.

A. 6 Laporan *State Of The Internet*

Indonesia berada di urutan kedua dalam daftar lima besar negara asal serangan kejahatan siber atau *cyber crime*, berdasar laporan State of The Internet 2013. Wakil

[14] Muladi 2002

Direktur Tindak Pidana Ekonomi Khusus Bareskrim Polri Kombespol Agung Setya mengatakan, dalam kurun waktu tiga tahun terakhir, tercatat 36,6 juta serangan *cyber crime* terjadi di Indonesia.Hal ini sesuai dengan data Security Threat 2013 yang menyebutkan Indonesia adalah negara paling berisiko mengalami serangan *cyber crime*.Sejak 2012 sampai dengan April 2015, Subdit IT/ *Cyber Crime* telah menangkap 497 orang tersangka kasus kejahatan di dunia maya.Dari jumlah tersebut, sebanyak 389 orang di antaranya merupakan warga negara asing, dan 108 orang merupakan warga negara Indonesia.Total kerugian *cyber crime* di Indonesia mencapai Rp 33,29 miliar. "Angka ini jauh lebih besar dibandingkan perampokan nasabah bank secara konvensional," kata Agung di Jakarta, Senin (11/5/2015).Sementara itu, sepanjang 2012 sampai dengan 2014, terdapat 101 permintaan penyelidikan terhadap kasus *fraud* atau penipuan dari seluruh dunia. "Ini artinya, setiap 10 hari terdapat satu kejadian selama tiga tahun terakhir," ujar Agung.

A. 7 Laporan Akamai

Serangan cyber yang berasal dari indonesia dilaporkan meningkat. Bahkan kini mengambil porsi terbesar serangan cyber dunia yang sebelumnya dikuasai china. Dibandingkan pada kuartal pertama 2013, hingga akhir kuartal kedua 2013 ini jumlah serangan yang berasal dari indonesia meningkat dua kali lipat. Berdasarkan laporan keamanan yang dirilis akamai, indonesia kini mengantongi porsi terbesar serangan dengan perolehan 38%,naik 17% dari peroide sebelumnya.Sedangkan china yang sebelumnya mendominasi kini hanya memiliki porsi 33%. Akamai menegaskan bahwa ini bukan berarti bahwa para penyerang itu memang benar dari indonesia. Karena pada dasarnya, para peretas bisa saja menggunakan alamat IP wilayah lain untuk menghilangkan jejak.[15]

[15] www.detiknet.com

Berikut adalah 10 negara dengan serangan cyber terbesar

	Country	Q2 '13 % Traffic	Q1 '13 %
1	Indonesia	38%	21%
2	China	33%	34%
3	United States	6.9%	8.3%
4	Taiwan	2.5%	2.5%
5	Turkey	2.4%	4.5%
6	India	2.0%	2.6%
7	Russia	1.7%	2.7%
8	Brazil	1.4%	2.2%
9	Romania	1.0%	2.0%
10	South Korea	0.9%	1.4%
–	Other	11%	18%

Figure 1: Attack Traffic, Top Originating Countries (by source IP address, not attribution)

Gambar 2.1 Negara Serangan Cyber

Sumber (www.detiknet.com)

A. 8 Laporan ID-SIRTII

Isu kemanan siber yang kini memang menjadi pehatian banyak pihak, termasuk pemerintah. ID-SIRTII (*Indonesia Security Incident Response Team On Internet Infrastructure)* mengatakan bahwa sepanjang tahun 2014, setidaknya terjadi 48,4 juta serangan keamanan siber dalam berbagai bentuk, termasuk serangan ke situs tertentu atau penyebaran malware melalui berbagai teknik. Informasi ini disampaikan langsung oleh Ketua ID-SIRTII Rudi Lumanto saat menjadi salah satu pembicara utama dalam *Virtus Security Day* 2015.

Dia menjelaskan, puluhan juta serangan yang muncul tahun lalu ini ternyata bukan berasal dari hacker atau oknum lain di luar negeri. “60 persen serangan ternyata berasal dari Indonesia sendiri, bukan dari luar negeri,” katanya di hadapan para tamu undangan, Kamis (30/4/2015). Dari gambar di bawah, kita bisa melihat bahwa di tahun 2014, Indonesia memiliki sekitar 12 juta aktivitas malware, dengan 12 ribu merupakan insiden website. Dari jumlah 12 ribu ini, setidaknya ada 3 ribu serangan siber terhadap situs pemerintah alias yang menggunakan domain .go.id. “Secara index, Indonesia memiliki kekuatan siber cukup tinggi, yaitu peringkat 13 di dunia, dan peringkat 5 di Asia Pasifik.”Peringkat kemanan siber ini memiliki lima kriteria berdasarkan Global Cyber Security Index (ITU, ABI Research),

yaitu Legal, Teknis, Kelembagaan, Peningkatan Kapasitas, dan Kerja Sama. Kolaborasi menjadi satu aspek yang ditekankan oleh ID-SIRTII, salah satunya adalah dengan mengadakan pelatihan keamanan siber secara rutin tanpa dipungut biaya. "Biasanya pelatihan *security* itu harganya mahal." imbuhnya.Sambil memberikan data statistik terkait keamanan siber Indonesia, dia juga menjelaskan bahwa secara global, dalam satu menit terdapat 20 unit PC yang mengalami kebocoran data, ditambah dengan 416 uji coba serangan. Jumlah ini bisa terus meningkat jika perusahaan tidak mengimbanginya dengan sistem keamanan yang diperbarui secara rutin.[16]

Gambar 2.2 (Serangan Cyber Indonesia 2014)

Sumber (Metronews.Com)

A. 9 Laporan Dirjen Imigrasi

Direktorat jendral imigrasi kementrian hokum dan HAM mencatat 300 kasus kejahatan siber *(cyber crime*) yang diduga dilakukan oleh warga negara di indonesia pada paruh pertama 2015. Hal tersebut disampaikan oleh direktur jendral imigrasi ronny sompie dikantornya, dia menagatakan warga asing itu menggunakan indonesia sebagai basis operasi untuk melakukan penipuan di luar negeri. Dia juga menagatakan selain pengawasan oleh petugas keimigrasian, diperlukan juga kerjasama masyarakat untuk mengungkap pelanggaran imigrasi seperti ini. Kendala utama yang dialami oleh pihak imigrasi adalah minimnya informasi yang disampaikan oleh masyarakat.

[16] http://teknologi.metrotvnews.com/read/2015/04/30/121209/tahun-2014-situs-pemerintah-target-utama-serangan-siber

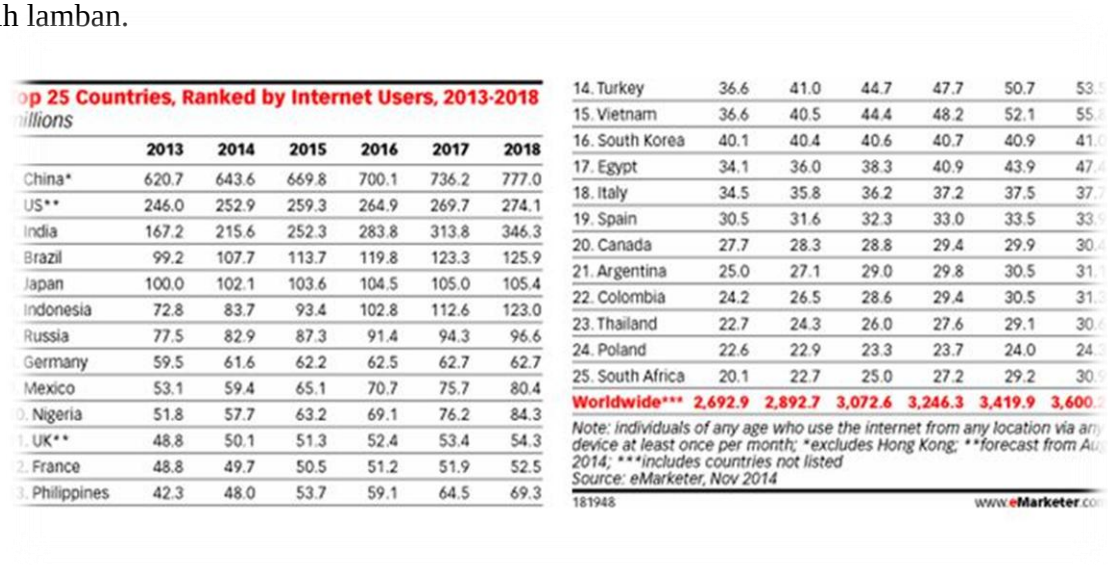
48 warga Negara asing telah ditangkap di bali karena dugaan pelanggaran imigrasi, puluhan warga china dan Taiwan itu juga diduga melakukan *cyber crime.* khusus di bali yang menjadi kendala adalah banyak masyarakat yang menyewakan rumahnya untuk dijadikan sumber pemasukan. Pemilik rumah tidak selalu melaporkan ketidaklengkapan dokumen ke petugas. Mudahnya warga Negara asing di Indonesia masuk ke wilayah Indoensia merupakan dampak dari kebijakan pemerintah untuk memebrlakukan pembebasan visa, pada tahun 2016 saja dibawah presiden joko widodo, sudah memberlakukan kebijakan bebas visa kepada 169 negara berdasarkan peaturan presiden nomor 21 tahun 2016. Berbagai macam laporan seperti yang tertera diatas, penulis menyimpulkan bahwa serangan *cybercrime* di Indoensia semakin lama semakin meningkat. Serangan tersebut diantaranya berupa *Malware* atau virus yang begitu banyak menargetkan situs situs pemerintah. Bisa kita lihat pada tahun 2014 seperti yang telah disampaikan oleh ID-SIRTII target yang beralamat .go.id mendapat jumlah serangan sebanyak 3.288 serangan.

Serangan-serangan yang terjadi di indonesia tidak lepas dari para pengguna internet indonesia, berdasarkan data yang didapat oleh penulis dari Asosiasi Penyedia Jasa Internet Indonesia (APJII) telah merilis hasil riset nasional terkait jumlah pengguna dan penetrasi internet di indonesia untuk pengguna internet pada tahun 2014 mencapai 88,1 juta sedangkan pada tahun 2013 mencapai 71,9 juta pengguna maka pengguna intenet di indonesia mengalami peningkatan sekitar 16,2 juta jiwa. Pengguna internet di indonesia paling banyak terkonsentrasi di pulau jawa dan bali sebanyak 53 juta pengguna.

penetrasi paling tinggi ada di kota Jakarta dengan presentase 65% disusul oleh DI Yogyakarta yang memiliki presentase 63% sedangkan wilayah timur di papua hanya 20% dari jumlah populasinya yang menggunakan internet.[17] Sedangkan untuk peringkat dunia indonesia menempati posisi 6 berdasarkan sumber dari lembaga riset pasar e-marketer, secara keseluruhan, jumlah pengguna internet di seluruh dunia diproyeksikan mencapai 3 miliar orang pada tahun 2015.

[17] http://tekno.liputan6.com.jumlah-pengguna-internet-indonesia-capai-881-juta
Di akses pada tanggal 26-april-2016

Tiga tahun kemudian pada tahun 2018 diperkirakan akan mencapai 3,6 miliar pengguna di dunia akan menggunakan akses internet. Prediksi lain dari e-marketer pada tahun 2017 memperkirakan jumlah netter indonesia akan menacapai 112 juta orang, mengalahkan jepang pada peringkat ke 5 yang pertumbuhan jumlah pengguna internetnya lebih lamban.



p 25 Countries, Ranked by Internet Users, 2013-2018
illions

	2013	2014	2015	2016	2017	2018
China*	620.7	643.6	669.8	700.1	736.2	777.0
US**	246.0	252.9	259.3	264.9	269.7	274.1
India	167.2	215.6	252.3	283.8	313.8	346.3
Brazil	99.2	107.7	113.7	119.8	123.3	125.9
Japan	100.0	102.1	103.6	104.5	105.0	105.4
Indonesia	72.8	83.7	93.4	102.8	112.6	123.0
Russia	77.5	82.9	87.3	91.4	94.3	96.6
Germany	59.5	61.6	62.2	62.5	62.7	62.7
Mexico	53.1	59.4	65.1	70.7	75.7	80.4
Nigeria	51.8	57.7	63.2	69.1	76.2	84.3
UK**	48.8	50.1	51.3	52.4	53.4	54.3
France	48.8	49.7	50.5	51.2	51.9	52.5
Philippines	42.3	48.0	53.7	59.1	64.5	69.3
14. Turkey	36.6	41.0	44.7	47.7	50.7	53.
15. Vietnam	36.6	40.5	44.4	48.2	52.1	55.
16. South Korea	40.1	40.4	40.6	40.7	40.9	41.
17. Egypt	34.1	36.0	38.3	40.9	43.9	47.
18. Italy	34.5	35.8	36.2	37.2	37.5	37.
19. Spain	30.5	31.6	32.3	33.0	33.5	33.
20. Canada	27.7	28.3	28.8	29.4	29.9	30.
21. Argentina	25.0	27.1	29.0	29.8	30.5	31.
22. Colombia	24.2	26.5	28.6	29.4	30.5	31.
23. Thailand	22.7	24.3	26.0	27.6	29.1	30.
24. Poland	22.6	22.9	23.3	23.7	24.0	24.
25. South Africa	20.1	22.7	25.0	27.2	29.2	30.
Worldwide* **	**2,692.9**	**2,892.7**	**3,072.6**	**3,246.3**	**3,419.9**	**3,600.**

*Note: individuals of any age who use the internet from any location via an device at least once per month; *excludes Hong Kong; **forecast from Au 2014; ***includes countries not listed*
Source: eMarketer, Nov 2014
181948 www.eMarketer.co

Gambar Tabel 2.3 Statistik Pengguna Internet Dunia

Sumber (*E-Marketer*)

B. Karakteristik Pelaku Dan *Cyber Crime* Di Indonesia

Cyber crime memiliki bentuk beragam, karena setiap Negara tidak selalu sama dalam kriminalisasi. Begitu pula dalam setiap Negara menyebut apakah suatu perbuatan tergolong kejahatan "*cyber crime*" atau bukan kejahatan "*cyber crime*" juga belum tentu sama. Secara teoritik, berkaitan dengan konsepsi kejahatan Muladi mengemukakan bahwa asas *mala in se* mengajarkan bahwa suatu perbuatan dikategorkan sebagai kejahatan karena masyarakat dengan sendirinya mengangap perbuatan tersebut jahat. Sedangkan berdasarkan asas *mala prohibita* suatu perbuatan jahat karena melanggar peraturan perundang-undangan.[18] Karakterisitk selanjutnya yang merupakan ciri khas pelaku kejahatan *cyber crime* di Indoensia merupakan usia muda dari golongan terdidik dan terpelajar seperti mahasiswa. Seperti yang pernah terjadi sebelumnya di Indonesia kasus pembobolan situs KPU pada tahun 2004 pelaku pembobolan yang bernama Dany Firmansyah termasuk seorang yang terpelajar dia merasa tertantang dengan pernyataan resmi oleh pengelola situs

KPU tahun 2004 bahwa biaya untuk keamanan dari situs KPU tersebut memakan biaya hingga puluhan miliar rupiah. Begitu juga dengan pembobolan situs presiden RI yang ke 6 SBY (Susilo Bambang Yudhoyono) yang telah diretas oleh seorang pemuda asal jember jawa timur yang menamakan jember *hecker*. Fakta-fakta kasus tersebut teah membuktikan dengan nyata bahwa pelaku *cyber crime* di indonesia merupakan golongan terpelajar dan berusia muda.

B. 1 **Ragam Bentuk *Cyber Crime***

Secara umum, Ari Juliano Gema mengemukakan *cyber crime* dapat di kelomkpokan dalam bentuk sebagai berikut:

1. *Anuthorized access to computer system and service*

Kejahatan ini dilakukan dengan cara memasuki atau menyususp secara tidak sah kedalam suatu sistem atau jaringan computer.tujuan dari perbuatan tersebut adalah sabotase atau pencurian data atau pemalsuan informasi penting dan rahasia. Ciri utama dari perbuatan ini adalah memasuki system secara tidak sah. Apakah seseorang setelah memasuki kemudian melakukan perbuatan lanjutan yang merugikan korban atau tidak, bukan merupakan unsure yang menetukan kejahatan.

2. *Ilegal Contents*

Kejahatan ini dilakukan dengan jalan memasukan data atau informasi ke dalam jaringan internet tentang semua hal yang tidak benar, tidak etis dan dapat melanggar hukum atau ketertiban umum. Perbuatan tersebut misalnya pemuatan berita bohong, fitnah, pornogrrafi, pembocoran rahasia Negara, agitasi dan propaganda untuk melawan pemerintahan yang sah. Unsur utama pada kejahatan ini adalah pada “isi” data yang dimasukan ke dalam jaringan komputer.

3. *Data Forgery*

Kejahatan ini dilakukan dengan cara memalsu data pada dokumen-dokumen penting yang tersimpan dalam sistem komputer sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen perdagangan elektronik (e*commerce*) dengan cara memebuat pesan seolah-olah terjadi kesalahan pengetikan yang

dapat menguntungkan pelaku, karena korban sudah terlanjur memasukan data pribadi dan PIN kartu kredit sehingga pelaku memungkinkan menyalahgunakan data tersebut.

4. *Cyber Espionage*

Kejahatan ini dilakukan dengan jalan memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata (spionase) terhadap pihak lain dengan cara memasuki sistem jaringan komputer (*computer network system*) pihak lain. kejahatan ini biasanya ditujukan kepada orang atau saingan perusahaan bisnis yang dokumen atau data rahasia (*data base*) tersimpan dalam suatu sistem komputer yang tersambung ke jaringan komputer.

5. *Cyber Sabotage and Extortion*

Kejahatan ini dilakukan dengan cara membuat gangguan, perusakan atau penghancuran terhadap data, program atau sistem jaringan komputer yang terhubung dengan internet secara tidak sah. Kejahatan ini dilakukan dengan cara menyusupkan suatu *logic bomb*, virus komputer atau suatu program tertentu, sehingga data program atau sistem jaringan komputer tidak dapat digunakan, tidak dapat beroperasi sebagaimana mestinya, atau dapat beroperasi tetapi tidak sesuai dengan kehendak pelaku kejahatan.

Dalam beberapa kasus setelah kejahatan tersebut terjadi pelaku atau komplotan pelaku menawarkan jasa kepada korban untuk memperbaiki data atau program atau sistem jaringan komputer yang telah disabotase. Dengan meminta bayaran tertentu. Dengan demikian pelaku dan komplotanya memperoleh keuntungan secara ekonomi.

6. *Offense Against Intellectual Property*

Kejahatan jenis ini ditunjukan terhadap Hak Kekayaan Intelektual (HAKI) yang dimiliki oleh pihak lain di internet sebagai contoh adalah penjiplakan tampilan pada *web page* suatu situs milik orang lain secara illegal, penyiaran suatu informasi di internet yang merupakan rahasia dagang milik pihak lain.

7. *Infrigments Of Privacy*

Kejahatan jenis ini ditunjukan terhadap data atau informasi seseorang yang bersifat individual dan rahasia (*privacy*) secara melawan hukum. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada data formulir pribadi yang tersimpan secara *computerized*. Jika data tersebut diketahui oleh orang lain, dapat merugikan pemilik informasi baik secara materil maupun immaterial misalnya nomor kartu kredit, PIN, ATM, catatan-catatan pribadi, cacat tubuh, atau penyakit-penyakit tersembunyi.

Selain penggolongan *cyber crime* Donn Parker mengkalsifikasikan bentuk-bentuk *cyber crime* ke dalam 4 (empat) klasifikasi berikut.:

A. Komputer sebagai objek

   Dalam kategori ini, bentuk-bentuk *cyber crime* kasus kasusperusakan terhadap komputer, data atau program yang terdapat di dalamnya atau perusakan terhadap sarana-sarana komputer seperti *Air Conditioning* (AC) dan peralatan listrik yang menunjang pengoperasian komputer.

B. Komputer sebagai subjek

   Komputer dapat pula meni,bulkan tempat atau lingkungan untuk melakukan kejahatan, misalnya penipuan, pencurian dan pemalsuan yang menyangkut harta benda dalam bentuk baru yang tidak dapat disentuh *(intangible*), misalnya pulsa elektronik dan guratan-guratan pita magnetis.

C. Komputer Sebagai Alat

   Komputer Digunakan Sebagai Alat Kejahatan sehingga peristiwa kejahatan tersebut adalah sangat kompleks dan sulit diketahui. Salah satu contoh seseorang pelaku kejahatan yang mengambil warkat-warkat setoran dan menulis nomer rekening pelaku dengan tinta magnetis pada warkat tersebut, kemudian meletakkan kembali di tempat semula. Nasabah yang akan memasukan uang akan mengambil dan mengisi warkat yang sudah dibubuhi nomer rekening pelaku kejahatan tersebut sebagai bukti penyetoran. Pada waktu computer memproses warkat-warkat nasabah, komputer secara otomatis akan mengkredit sejumlah uang pada rekening pelaku

kejahatan, setelah itu, pelaku kejahatan akan menarik uang dengan cek dari rekening sebelum para nasabah yang menyetor mengajukan complain ke bank.

D. Komputer Sebagai Simbol

Suatu Komputer dapat digunakan sebagai simbol untuk melakukan penipuan atau ancaman. Dalam katagori ini termasuk penipuan dalam Biro Jodoh yang menyatakan biro jodoh tersebut memakai komputer untuk membantu si korban mencari jodoh akan tetapi biro jodoh tersebut sama sekali tidak memakai komputer untuk keperluan tersebut.[19]

J.Sudama Sastraandaja juga menyatakan bahwa *cyber crime* dapat dikalsifikasikan dalam 5 bentuk berikut.

A. Kejahatan-kejahatan yang menyangkut data atau informasi komputer.
B. Kejahatan-kejahatan yang menyangkut program atau *software computer*
C. Pemakaian fasilitas-fasilitas komputer tanpa wewenang untuk kepentingan-kepentingan yang tidak sesuai dengan tujuan atau pengelolaan pengoperasianya.
D. Tindakan-tindakan yang mengganggu operasional komputer.
E. Tindakan perusakan terhadap peralatan komputer atau peralatan-peralatan yang berhubungan dengan komputer atau sarana sarana penunjangnya.

Andi Hamzah, menguraikan bahwa bentuk-bentuk kejahatan *cyber crime* diatas dapat dikaitkan dengan ketentuan-ketentuan dalam buku II KUHP Indonesia. Jika dibuat pervabdingan maka akan diperoleh deskripsi sebagaimana uraian berikut.

I. *Joy Computing*

Adalah perbuatan seseorang yang menggunakan komputer secara tidak sah atau tanpa ijin dari pihak yang berwenang dan penggunaanya melampaui kewenangngan yang dimiliki. Tindakan ini dapat dikategorkan sebagai tindakan pidana pencurian (Pasal 362 KUHP)

[19] J. Sudama Sastraandaja

II. *Hacking*

Adalah perbuatan berupa penyambungan saluran, yaitu dengan cara menambah terminal komputer baru pada sistem jaringan komputer tanpa ijin (dilakukan dengan melawan hukum) dari pemilik sah jaringan komputer. Tindakan ini dapat dikategorikan sebagai tindakan pidana, yaitu tindakan yang masuk tanpa wewenang masuk dengan memaksa ke dalam rumah atau ruang yang tertutup atau pekarangan atau tanpa haknya berjalan di atas tanah milik orang lain (pasal 167 dan pasal 551 KUHP)

III. *The Trojan Horse*

Adalah menambah, mengurangi atau mengubah instruksi pada sebuah program sehingga program tersebut selain menjalankan tugas yang semestinya juga akan melaksanakan tugas lain yang tidak sah sebagaimana yang dikehendaki pelaku kejahatan tindakan ini dikategorkan sebagai tindakan pidana penggelapan (pasal 372 dan pasal 374 KUHP) Apa bila kerugian yang dittimbulkan menyangkut keuangan Negara, tindakan tersebut dapat dikatagorikan dalam tindak pidana korupsi.

IV. *Data Leakgage*

Adalah tindakan pembocoran data rahasia yang diakukan dengan cara menulis data rahasia tersebut ke dalam kode-kode tertentu sehingga data dapat diabawa keluar sistem komputer tanpa diketahui oleh pihak yang bertanggung jawab terhadap data tersebut. Tindakan ini dapat dikategorikan sebagai tindak pidana terhadap keamanan Negara (pasal 112, 113,114, dan pasal 115 KUHP) dan tindak pidana membuka rahasia perusahaan atau kewajiban menyimpan rahasia profesi atau jabatan (pasal 332 dan pasal 323 KUHP)

V. *Data Diddiling*

Adalah suatu tindakan pelanggaran hukum yang mengubah validitas data. Perbuatan ini dilakukan dengan cara mengubah input atau output data. Tindakan ini dapat dikategorikan sebagai tindak pidana pemalsuan surat (Pasal 263 KUHP)

VI. Penyia-nyian Data Komputer

Penyia-nyian Data Komputer dapat diartikan sebagai suatu perbuatan yang dilakukan dengan sengaja untuk merusak atau menghancurkan media disket dan media penyimpanan sejenis lainya misalnya hardisc. Yang berisis data atau program komputer sehingga data atau program tersebut tidak berfungsi sebagaimana mestinya. Tindakan ini dapat dikategorikan sebagai tindak pidana perusakan barang (Pasal 406 KUHP)[20]

B. 2 Karakterisitk *Cyber Crime*

Ada perbedaan antara karakterisitk *cyber crime* dengan kejahatan karakterisitk konvensional, terutama pada sifat, tempat, alat, cara dan akibat. *Cyber crime* merupakan kejahatan transnasional, bertempat di dunia virtual (maya), menggunakan alat berteknologi tinggi (berbasis komputer) dengan cara yang bervariasi dalam jangka waktu yang singkat, dan akibatnya sangat banyak dan menjangkau wilayah yang sangat luas. Sedangkan kejahatan konvensional biasanya dilakukan secara lokal dalam spectrum nyata (*real*) menggunakan alat konvensional dan modusnya tidak banyak bervariasi. Akibat perbuatannya terbatas pada ruang dan waktu tertentu dengan korban yang tidak selalu banyak dan menjangkau wilayah yang luas. Ari Juliano Gema menjelaskan bahwa *computer related crime* memiliki karakteristik yang khas berbeda dengan kejahatan konvensional karakter tersebut adalah sebagai berikut.

1) Perbuatan yang dilakukan secara illegal, tanpa hak dan tidak etis tersebut terjadi di ruang wilayah maya (*cyber space*), sehingga sulit dipastikan yuridis hukum Negara mana yang dapat diberlakukan.
2) Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet, karena internet saat ini sudah memasuki internet generasi ke II, sebagai salah satu cirinya adalah media internet tidak hanya pada layar monitor komputer.
3) Perbuatan tersebut mengakibatkan kerugian yang jauh lebih besar dibandingkan dengan kejahatan konvensional, baik kerugian yang bersifat materil maupun

[20] Andi Hamzah JAKARTA 1996

immaterial (misalnya waktu, nilai, jasa, martabat, kebebasan dan kerahasian informasi).

4) Pelaku kejahatan adalah orang yang menguasai penggunaan komputer, internet beserta aplikasinya.
5) Perbuatan tersebut sering kali dilakukan secara transnasional/melintasi batas negara[21]

Berdsarakan jabaran di atas dapat pula dipahami bahwa ada perbedaan antara karaktersitk pelaku *cyber crime* dan karakterisitk *cyber crime*, karakterisitk pelaku kejahatan *cyber crime* juga berbeda dengan karakterisitk pelaku kejahatan tradisional. Secara kriminologis, faktor penyebab terjadinya *cyber crime* berbeda dengan kejahatan tradisional.

B. 3 Karakteristik *Cyber Crime* Di Indonesia

Berdasarkan hasil peneltitian Widodo, motivasi pelaku *cyber crime* di Indoensia adalah mencoba kemampuan dan keterampilan diri sendiri dalam mengoperasikan peralatan teknologi informasi menguji pihak lain yang mengelola dan mengamankan situs/*website*, bersenang-senang ingin dianggap sebagai pahlawan (*hero*) memperkenalkan atau mempopulerkan kelompok *hecker/cracker*, memperoleh uang, balas dendam, politik pelampiasan kekecewaan, dan persaingan usaha. Dalam satu bentuk kejahatan kemungkinan di dorong oleh lebih dari satu motivasi. Antara satu bentuk kejahatan dengan kejahatan lainya,mempunyai motivasi yang berbeda. Karena itu teori kriminologi tentang *Multipile Factor Theory* dapat digunakan sebagai pisau analisis penyebab pelaku *cyber crime* di Indonesia[22].

Karakteristik *cyber crime* di indoensia adalah sebagai berikut:

a) Bersifat lintas Negara (*Trans-National Crime*)
b) Bukan hanya menggunakan komputer konvensional (melainkan sudah menggunakan laptop, *hanphone*, tablet)

[21] Ari juliano Gema, cyber crime sebuah fenomena di dunia maya Majalah Infokom, p, 12
[22] Widodo 2006

c) Ada yang dapat digolongkan sebagai *white collar criminal* dan ada yang bukan *white collar criminal*

d) Bukan merupakan kejahatan organisasi

e) Dapat berupa kejahatan korporasi dan bukan kejahatan korporasi[23]

Sedangkan karakterisitk pelaku *cyber crime* di Indonesia adalah sebagai berikut

a) Mempunyai keterampilan yang sangat memadai dalam mengoperasikan komputer, internet, serta program aplikasinya

b) Berpendidikan relatif tinggi (termasuk mahasiswa)

c) Tinggal di kota-kota besar yaitu ibu kota kabupaten , provinsi, dan Negara

d) Memyukai tantangan di bidang teknologi informasi yang berbasis computer

e) Mayoritas berjenis kelmain laki-laki

f) Mempunyai kreatifitas yang tinggi dan ulet

g) Pandai memanfaatkan peluang yang ada untuk melakukan kejahatan dan mayoritas tergabung dalam komunitas *underground*[24]

Berkaitan Dengan Hasil Penelitian Widodo, ternyata berdasarkan pendapat Sue Titus Reid, secara umum ternyata *cyber crime* diluar Indonesia dapat dilakukan secara organisasi (*organized crime*) dan dapat dilakukan oleh orang-orang terhormat dengan cara menyalahgunakan wewenangnya (*white collar crime*). saat ini bahkan *cyber crime* memiliki karakterisitk yang semakin unik, karena pengguna *cyber space* sudah membentuk masyarakat tersendiri, yang lazim disebut *underground*. Lewat komunitas inilah para pengguna internet dapat saling berkomunikasi, berinteraksi di dunia maya, bahkan saling memberikan informasi yang mungkin dapat mengarah pada perbuatan jahat.

Meskipun pelaku kejahatan tersebut saling terikat dengan komunitas *Underground*, tetapi keterkaitan tersebut hanya sebatas komunikasi dan tukar menukar informasi melalui internet *(chatting*) sehingga tidak ada hubungan struktural dan fungsional sebagaimana ada dalam setiap organisasi formal. Menururt Agus Rahardjo dalam, dalam *cyber space* terdapat *whole world lectronic link (WELL*) yaitu sebuah tempat yang memungkinkan

[23] Ibid
[24] Ibid

orang-orang dari seluruh dunia saling berbicara atau bercakap-cakap untuk bertukar informasi.

B. 4 Motivasi Pelaku *Cyber Crime* Di Indonesia

Berdasarkan Hasil Wawancara Dengan Dicky Patrianegara, motivasi pelaku *cyber crime* sangat bervariasi, tergantung pada bentuk kejahatan yang dilakukan dengan karakterisitk pribadi pelaku kejahatan selanjutnya di uraikan sebagai berikut.

1. Saat ini ada perubahan motivasi dalam melakukan kejahatan. Jika dahulu para pelaku cracking, Dos atau *DDoS attack* atau kejahatan lain terhadap system atau jaringan komputer melakukan kejahatan karena merasa tertantang dengan teknologi, mencoba keaandalan pengaman sistem komputer pihak lain dan bersenang-senang. Saat ini banyak pihak yang melakukan aktifitas tersebut termotivasi karena perolehan imbalan berupa uang (motivasi ekonomi) saat ini sedang marak terjadi bahwa seorang *cracker* yang melakukan *cracking* atau *DDoS attack* karena diberi upah oleh seseorang yang tidak mampu melakukan *cracking*. Motivasi pihak yang membayar cracker antara lain balas dendam (karena situs miliknya pernah diserang), perdaingan usaha, untuk menegtahui rahasia dagang, atau mencari kelemahan pihak lain
2. Dalam kasus *typosquating*, pelaku kejahatan termotivasi oleh keinginan agara dalam pengguna e-banking dalam bertransaksi lebih berhati-hati dalam memasukan PIN dan identitas pengguna (user identity). Kasusu ini pernah terjadi pada *typosquating* bank BCA.
3. Dalam kasus-kasus atau kejahatan yang dapat mendatangkan keuntungan berupa uang, misalnya *carding*, penipuan melalui bank (transfer fiktif, transfer tanpa hak), korupsi, penyalah gunaan nama domain, pelanggaran hak cipta dan *phising*. Sebagian besar pelaku di dorongan oleh motif mendapatkan keuntungan berupa baik bagi diri sendiri maupun orang lain uang secara melawan hukum.
4. Motif politik juga dapat mendorong tindakan *cracking*, *defacing*, dan *Dos Attack*, misalnya pada saat antara Indonesia dan Malaysia sedang membicarakan status kepulauan ambalat tahun 2005. Motif kekecewaan sekelompok orang atau sekelompok *cracker* dapat memacu *cyber crime.*

C. Kriminalisasi Perbuatan Yang Menjadikan Komputer Sebagai Sasaran Kejahatan Di Indonesia

Kriminalisasi terhadap pelaku kejahatan yang menggunakan teknologi baik berupa komputer, alat komunikasi dan teknologi informasi pada umumnya perlu dilakukan oleh para penegak hukum, karena dengan adanya status kriminalisasi maka sudah dapat dipastikan bahwa pelaku kejahatan telah melakukan perbuatan yang merugikan orang lain, sebagai contoh perbuatan melakukan transaksi illegal, pembobolan kartu kredit ,nomor rekening, dan penipuan.

C. 1 Konspesi Kriminalisasi Perbuatan *Cyber Crime*

Berkaitan dengan upaya kriminalisasi, berikut akan dijabarkan tentang kriminalisasi bentuk-bentuk *cyber crime*, harmonisasi asubtansi atau materi dan harmonisasi formulasi *cyber crime* di indonesia. Sudarto berpebdapat kriminalisasi adalah proses penetapan suatu perbuatan orang sebagai sudatu tindak pidana. Proses tersebut diakhiri dengan adanya undang-undangyang mengatur bahwa perbauatan tersebut merupakan tindak [idana dan diancam dengan hukum pidana.

Pendapat serupa juga dikemukakan oleh Barda Nawawi Arief. Bahwa kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana) dalam kontek ini yang diamaksud dengan kriminalisasi "*cyber crime*" sebenarnya adalah perbauatan kriminalisasi perbuatan-perbuatan yang dilakukan dalam dunia *cyber*, karena istilah kriminalisasi *cyber crime* secara terminologis tidak tepat. Karena makna cyber crime adalah kejahatan di dunia maya (*space*) sehingga jika diguanakan istilah kriminalisasi *cyber crime* berarti mengkriminalkan kejahatan, bukan mengkriminalkan perbuatan. Penggunaa istilah krimiinalisasi dalam hukum pidana selalu menunjuk upaya menjadikan perbuatan yang bukan melanggar hukum, kemudian diubah oleh legislator menjadi perbuatan yang melanggar hukum dengan cara mengatur perbuatan tersebut dalam peraturan perundang-undangan. Dalam msayarakat masih sering terjadi kesalahan penggunaan istilah kriminalisasi, misalnya kriminalisasi KPK, dan kriminalisasi Pers.

Dalam melakjukan kriminalisasi perlu diperhatikan 4 hal berikut:

1. Penggunaan dalam hukum pidana perlu memperhatikan tujuan pembangunan nasional, yaitu mewujudkan masyarakat yang adil dan makmur yang merata baik yang spiritual dan material. Berdasarkan pancasila. Penggunaan hukum pidana ditujukan untuk menaggulangi kejahatan dan mengadakan peng-ungeran terhadap tindakan penanggulaangan itu sendiri, demi kesejahterraan dan pengayoman masayarakat.
2. Perbuatan yang disuahakan dicegah atau di tanggulangi dengan hukum pidana seyogyanya merupakan perbuatan yang tidak di kehendaki, yaitu perbuatan yang mendatangkan kerugian material atau spiritual pada warga masyarakat.
3. Penggunaan hukum pidana perlu memperhitungkan prinsip biaya dan hasil (*cost and benefit principal).*
4. Penggunaan hukum pidana perlu pula memperhatikan kepastian atau kemampuan daya kerja dari badan-badan penegak hokum pidana jangan sampai ada kelbihan beban tugas (*overbelasting)*[25].

Selain Itu, saat ini ada beberapa pelaku kasus cyber crime yang di motivasi oleh rasa ingin menampilkan kelucuan (*funny*) misalnya dalam kasus blogger yang sering dijumpai di internet, antara lain menyandingkan foto president Susilo Bambang Yudhoyono dengan Tommy Soeharto, menampilkan para tokoh-tokoh yang direkayasa sehingga melihat users penasaran, kasus ini belum tentu dapat dikatakan sebagai kasus kejahatan.[26] Menurut Avinata Tarigan dan I Made Wiryana motivasi para *hecker* untuk menemukan *vuneralibilty* adalah untuk membuktikan kemampuan pelaku dalam bidang teknologi informasi atau sebagai bagian dari sarana kontrol sosial terhadap suatu komputer pihak lain. sedangkan motivasi para *cracker* sangat beragam antara lain untuk propaganda (melalui *defacing* terhadap *website)* penyerangan destruktif (diseabakan oleh perasaan dendam atau ketidaksukaaan terhadap suatu institusi tertentu) dan lain-lain[27].

[25] Sudarto Hukum Pidana Bandung 1981
[26] Widodo 2006
[27] Avianata Tarigan Dan I Made Irwayana 2006

Berdasarkan hasil identifikasi beberapa kasus dan wawancara dengan penyidik *Cyber Crime* Mabes Polri, motivasi utama pelaku *cyber crime* di bidang perbankan di indoensia misalnya banking *fraud corruption*, adalah memperoleh uang. Hasil temuan ini berbeda dengan hasil penelitian yang dikemukakan oleh Aman Nursusila, bahwa faktor penyebab terjadinya *cyber crime* di bidang perbankan adalah mencoba kemampuan di bidang Teknologi Internet (66,6%), dan karena motif ekonomi (33,3%), perbedaan ini dapat dipahami karena kedua penelitian tersebut dilakukan dalam waktu, lokasi dan kasus yang berbeda. Menurut beberapa hasil pengamatan dan riset yang dilakukan oleh *Information* Dan *Communication Technology* (ICT) *Watch* terhadap komunitas maya *underground* di indoensia. Ada beberaa penyebab terjadinya *cyber crime* di Indoensia, khususnya *Cracking*. Penyebab tersebut disingkat dengan formulasi 3M+M2, yaitu Motivasi, Mekanisme, Momentum Dan Miskonsepsi.[28]

C. 2 Motivasi

Motivasi adalah rangsangan yang berasal dari pengaruh teman pergaulan (peer group), baik secara internal maupun ekstrnal pengertian motivasi internal adalah dorongan yang berasal dari dalam komunitas atau kelompok pelaku, misalnya ajakan, hasutan atau pujian antar sesama rekan di komunitas maya (*underground*) sedangkan motivasi ekternal adalah dorongan berupa semangat bersaing antar kelompok, keinginana menjadi terkenal dan motivasi *hecktivitisme.*

Suatu reaksi yang yang dilatar belakangi semangat oleh para *hecker* atau *cracker,* untuk melakukan protes terhadap suatu kondisi politik atau social yang dihadapi. Motivasi eksternal lainya berupa tantangan atau kesombongan dari pihak tertentu atas jaminan kemanan suatu sistem atau jaringan komputer, tantangan eksternal tersebut dapat membangkitkan adrenalin rasa keinginantahuan seorang cracker. Rasa ingin tahu yang tinggi mnerupakan ciri khas yang inheren dalam komunitas underground. Motivasi eksternal sebagai penyebab motivasi kejahatan dapat dibuktikan dari pengakuan dani firmansyah (terpidana(*cracker)*

situs milik komisi pemilihan umum) yang sebagaimana ditulis dalam berita acara penyelidikan (BAP) bahwa ia merasa tertantang setelah mendengar pernyataan ketua

[28] Donny Budi Utoyo 2004

kelompok kerja teknologi informasi komisi pemilihan umum (KPU), Chusnul Mar'iyah, pada sebuah tayangan di televisi yang menyatakan bahwa sistem teknologi informasi komisi pemilihan umum di Indonesia di tahun 2004. Menghabiskan dana bernilai Rp.152.000.000.000,00 (Seratus Lima Puluh Dua Milyar Rupiah), sehingga sangat aman dan tidak bisa ditembus oleh *hacker.* Menurut Dani, pembobolan situs KPU tersebut adalah untuk menguji sistem keamanan server penghitungan suara di KPU. Ternyata sistem keamanan KPU mampu ditembus oleh *Cracker* secara mudah.

C. 3 Mekanisme

Kelemahan mekanisme pertahanan atau pengamanan server atau *website* juga menjadi penyebab kejahatan (*kriminogen*), misalnya karena tidak di *update* atau tidak di *patched* secara rutin dan menyeluruh. Banyak pengelola situs di Indonesia tidak melakukan peninjuan sistem pengamanan jaringan komputer secara rutin. Kelemahan tersebut dianggap sebagai peluang cracker untuk melakukan defacing atau kejahatan *cyber crime* bentuk lainya.

Bahkan, saat ini sudah tersedianya mekanisme sekunder berupa program (*software*) yang dapat berfungsi untuk mendeteksi kelemahan suatu system di internet, yaitu berupa *exploit software,* perangkat-perangkat tersebut tersedia di internet dan mudah ditemukan kemudian digunakan oleh para *cracker,* termasuk oleh para *cracker* pemula kelemahan pengamanan sistem atau jaringan komputer sebagai penyebab *cyber crime* di Indonesia juga dikemukakan oleh bebrapa ahli teknologi informasi, antara lain Agus Rahardjo.

C. 4 Momentum

Pengertian Momentum ialah isu-isu yang tengah menjadi sorotan atau polemik masyarakat luas, ini dianggap sebagai media yang tepat oleh *cracker* untuk menjalankan aksi *cracking* atau *defacing* atau bahkan *DoSS Attack*, jika *cracker* berhasil melakukan aksi kejahatan, maka akan dapat ter-ekspos secara luas di media massa atau internet, sebagai contoh pada tahun 2002 para *cracker* Indonesia menumpang isu ketegangan hubungan diplomatik antara Indonesia dengan Austarlia, yaitu dengan melakukan *cracking* ke sejumlah *website* yang beralamat di Australia yang isinya cemoohan terhadap pemerintah Australia. Pada tahun sebelumnya para *cracker* melakukan penyerangan terhadap situs

Ajinomoto yang sedang dikabarkan bahwa produk poenyedap rasa tersebut menagndung lemak babi yang haram di konsumsi umat islam.

C. 5 Miskonsepsi

Adalah ulasan mengenai keberadaan cracker dan aktifitasnya di media massa. Hal ini justru dimanfaatkan oleh para *cracker* agar terkenal atau memperkenalkan kelompoknya misalnya, *Cracker Fabianclone*. Selain itu, para *cracker* juga ingin dianggap sebagai seseorang yang heroik dan mempunyai nasionalisme yang tinggi.[29] Contoh kasus ini adalah serangan *cracker* indonesia terhadap situs luar negeri secara terang-terangan ikut memperjuangkan kemerdekaan Timur-Timor pada tahun 1998, pada tahun 2013, Wildan Yani Ashari alias yayan dari kota Jember, terpidana kasus *hacking* milik presiden RI Susilo Bambang Yudhoyono (WWW.Presidensby.info) juga mencantumkan "*Jember Hacker Team*"

Selain unsur pengamanan sistem atau jaringan komputer yang kurang memadai, *cyber crime* juga disebabkan oleh sifat kejahatan tersebut, yaitu ada dalam lingkup dunia maya (*virtual)* dan bersifat transnasional sehingga lebih mudah dilakukan dibandingkan dengan kejahatan konvensional di dunia nyata *(real*), dan lebih mudah pula menghilangkan jejak kejahatan. Kecerobohan operator atau programmer dalam mengoperasikan sistem atau jaringan komputer, *Internet Service Provider (ISP*) tidak membuat registrasi dan rekaman secara memadai untuk mendeteksi kejahatan, warung *internet* atau *Café Internet* yang tidak mendata pengguna *internet* secara cermat juga merupakan kriminogen.[30] Berdasarkan identifikasi kasus *cyber crime* di Mabes Polri dan hasil wawancara dengan penyidik tentang motivasi pelaku kejahatan *cyber crime* di Indoensia pada akhir tahun 2005 mengaitkan antara motivasi pelaku *cyber crime* dengan bentuk kasus yang terjadi di Indonesia. Motivasi dan bentuk kejahatan tersebut adalah sebagai berikut.

a) Mencoba kemampuan dan keterampilan diri sendiri dalam mengoperasikan peralatan dan teknologi informasi. Hal ini terjadi pada sebagian besar bentuk *cyber crime.*

[29] Donny Budi Utoyo 2004
[30] Widodo 2006

b) Menguji pihak lain yang mengelola situs/web site, misalnya dalam kasus *hacking* situs KPU oleh Danny Firmansyah (2004)
c) Bersenang-senang misalnya pada kasus *defacing* di beberapa situs
d) Ingin dianggap sebagai pahlawan (*hero),* misalnya pada beberapa kasus *hacking* pada situs ke *Website Connect Ireland* yang dianggap ikut memeprjuangkan kemerdekaan Timor Timur tahun 1998.
e) Memperkenalkan atau mempopulerkan kelompok *hecker,* misalnya dalam kasus *hecking* ke situs Bursa Efek Jakarta (BEJ) *Bank Central Asia* (BCA) dan Indosat net yang dilakukan oleh *hecker* yang menyebut dirinya *fabianclone* dan *naisenodni* tahun 2000
f) Memperoleh uang dengan secara tidak sah, misalnya dalam kasus *banking fraud* di BCA cabang purwokerto tahun 2001 dan *carding* di beberapa daerah.
g) Balas dendam, misalnya *crecker* yang di duga berasal dari cina yang menyebut dirinya *discover*, mengacak-acak situs milik Badan Koordinasi Keluarga Berencana Nasional (BKKBN) serangan ini merupakan reaksi atas pemeberitaan media masa mengenai kerusuhan pada bulan mei 1998 di Jakarta yang mengakibatkan beberapa orang etnis cina di Indonesia menjadi korban pembantaian dan pemerkosaan. Serangan tersebut juga dibalas oleh *cracker* Indonesia dengan merusak beberapa situs di Republic Rakyat Cina.
h) Motif politik, misalnya dalam kasus cracking yang dilakukan *crecker* indonesia ke *Website Connect Ireland* dan ancaman melalui internet terhadap Perdana Menteri Australia.

D. Karakteristik Pelaku *Cyber Crime* Di Indonesia

Berdasarkan hasil identifikasi kasus dalam daftar kasus *cyber crime* di unit V infotek*/cybercrime* Mabes Polri, diketahui bahwa kejahatan tersebut dilakukan dengan menggunakan protokol internet di kota kota besar yaitu Jakarta, Yogyakarta, Bandung, Semarang Surabaya, Medan Batam, Denpasar Malang, Pasuruan, Mataram dan Makasar. Delapan puluh lima persen (85%) pelaku *cyber crime* di Indonesia berjenis kelamin laki-laki dan lima belas persen (15%) berjenis kelamin perempuan.

Beberapa pelaku tergolong anak-anak (berusia kurang dari 18 tahun). Hasil identifikasi ini selaras dengan uraian Suheimi bahwa pada sekitar tahun 1990-an, Sembilan puluh persen (90%) pelaku *cyber crime* di Amerika Serikat juga berjenis kelamin laki-laki.[31] Berdsarkan dengan ciri pelaku kejahatan, semua pelaku *cyber crime* (kecuali orang yang membujuk atau turut serta melakukan kejahatan) mahir megoerasikan komputer dan program-program aplikasinya, menyukai tantangan di bidang teknologi dan informasi.

secara informal tergabung dalam msayarakat *cyber space* (*underground*), kreatif, berkemauan kuat dan usia yang relatif masih muda[32] selanjutnya dikemukakkan bahwa pelaku mempunyai pendidikan relatif tinggi (termasuk mahasiswa), gemar melakukan *chatting* dan berjenis kelamin laki laki.[33] Berdasarkan paparan tersebut diketahui bahwa karakterisitk pelaku *cyber crime* di indoensia dalah sebagai berikut.

a) Mayoritas berjenis kelamin laki-laki
b) Tinggal di kota-kota besar, yaitu ibukota kabupaten, provinsi dan ibu kota Negara
c) Mempunyai ketermapilan yang sangat memadai dalam mengoperasikan komputer, internet serta program aplikasinya
d) Berpendidikan relatif tinggi (termasuk mahasiswa)
e) Menyukai tantangan di bidang teknologi informasi yang berbasis komputer
f) Mempunyai kreatifitas yang tinggi *ulet*
g) Pandai memanfaatkan peluang yang ada untuk melakukan kejahatan
h) Mayoritas tergabung dalam komunitas *underground*

Karakterisitk pelaku *cyber crime* di Indonesia sebagaimana terjabar seperti yang di atas sama dengan isi *A National Criminal Justice Information And Statistic Service Report Of The Law Enforcement Assistance Administration* berikut.

…The Following Characteristic, Which Are Similar To Those Of The Median Age Is Twenty Five Years. With A Range Of Eighteen To Forty Six Years. Such Younger People May Not Yet Be Assimiliated To The Ethic, And The Organization Of Their Profession, And They Have Often Been Trained In Collage And University Campuses Where Attacking

[31] Suheimi 1990
[32] Widodo 2006
[33] Ibid

Campus Computer System Is Not Only Condoned But Often Encouraged As An Educational Activity.

Karakterisitk khusus bahwa pelaku *cyber crime* selalu mempunyai ketrampilan tertentu dalam bidang computer masih merupakan suatu topic yang kontroversial beberapap ihak masih mengklaim bahwa tingkatan keterampilan bukan merupakan suatu indikator utama pelaku *cyber crime*, di pihak lain mengakui bahwa pelaku *cyber crime* yang berpotensi adalah mereka yang cerdas, gembira, bermotivasi tinggi dan berkeinginan menerima tantangan teknologi. Beberapa karakteristik ini sangat diinginkan karyawan dalam bidang-bidang pengolahan data elektronik. Pelaku kejahatan berumur antara 10 tahun sampai dengan 60 tahun memiliki keterampilan tidak sebagaimana kebanyakan orang mereka memiliki kemampuan bakat dan kemampuan unik, termotivasi oleh tantangan teknis, mempunyai potensi untuk mencari keuntungan, menginginkan kemahsyuran atau balas dendam atau juga untuk mempromosikan ideologi.

D. 1 Jaringan Sindikat *Cyber Crime* Internasional Di Indonesia

Jaringan sindikat *cyber crime* di Indoensia tidak hanya dilakukan oleh warga Negara indonesia saja namun juga dimanfaatkan oleh sindikat jaringan cyber crime internasional, semenjak diberlakukan UU ITE 2008 oleh pemerintah indonesia antara kurun waktu 2011 himgga 2015 ditemukan banyak kasus oleh pihak mabes polri dengan diungkapnya kasus penipuan dan pemerasan yang paling banyak dilakukan oleh sindikat dari Nigeria dan cina atau Tiongkok.

D. 2 Sindikat *Cyber Crime* Nigeria

Tiga pelaku *cyber crime* jaringan internasional, asal Nigeria Yakni Igue Chuku Augistin (32 Tahun), Ohakguherbert (32 Tahun), dan mahasiswa universitas Paramita, Karawaci Devi Irnasari (27 Tahun), tertangkap Di Komplek Vila Serpong, Blok D III No. 10 Rt 59/10 Jalan Purimoro III, Jelupang Kota Tangerang Selatan (Tangsel). Penagkapan pertama ketiga pelaku cyber crime itu, langsung dipimpin kasat cyber crime polda metro jaya ajun komisaris besar polisi (AKBP) hermawan. Dari tangan tersangka , petugas berhasil mengamankan sejumlah barang bukti seperti *laptop, modem* dan *handphone* yang dilakukan untuk melakukan transaksi jual beli lewat internet. kasat *cyber crime* Polda Metro Jaya AKBP Hermawan mengatakan, pelaku sangat menguasai internet dan

terorganisasi dengan baik. Bukan hanya di Indonesia, tapi juga dibantu oleh orang asing juga tentang bagiaman menata dan mengatur startegi menarik orang agar orang terpengaruh mengikuti keinginan mereka. "jadi intinya mereka ini melakukan penipuan melalui internet dengan menawarkan macam-macam barang dan jasa. Seperti *handphone, laptop* dan barang yang lebih besar pun mereka melayani seperti kamera. Dan orang yang sudah memberikan uang, bahkan ada yang dampai ratusan juta barangnya tidak pernah sampai".

Dalam melakukan transaksinya, tersangka meenggunakan akun social facebook dan jejaring sosial lainya yang tersedia di internet. Kedua warga Negara asing (WNA) itu, datang ke Indonesia dengan enggunakan visa sebagai pengusaha. Sedangkan tersangka lainya warga Negara Indonesia (WNI) berperan sebagai penghubung yang tugasnya meyakinkan pembeli. "untuk menipu korban, tersangka menggunakan HP saya yakin jika dihubungkan engan nomor *handphone* dan nomor rekening yang ada kasus ini akan terungkap. Kita masih mendalami kasus ini karena baru pertama kali ditangkap". Ditambahkan peran tersangka WNI dalam kasus *cyber crime* itu cukup besar karena keahlian berbahasa Indonesia dan Inggrisnya yang baiklah, tersangka yang menagku masih kuliah itu meyakinkan pembelinya lewat *hanpdhone*, dapat dijerat Dengan Undang-Undang Informasi Dan Transaksi Elektronik dan *money laundry* dengan hukuman pidana lima tahun penjara.

D. 3 Sindikat *Cyber Crime* Cina (Tiongkok)

Subdirektorat *cyber crime* yang bernaung di direktorat mencatat, jumlah laporan kejahatan cyber tahun 2012 hanya 781 laporan. Dari jumlah tersebut, hanya 86 laporan yang berhasil diselesaikan. Tahun 2013 jumlah laporan melonjak menjadi 1.347 laporan dengan penyelesaian laporan sebanyak 115 saja. Adapun, pada tahun 2014 terdapat 1.324 laporan dengan penyelesaian perkara sebanyak 307. Sementara sepanjang januari hingga oktober 2015, terdapat 1.325 laporan dengan jumlah perkara yang diselesaikan sebanyak 355. Diantara jumlah laporan dan data yang didapat adapaun beberapa kasus yang berhasil diungkap oleh tim mabes polri dalam memberatntas sindikat *cyber crime* Cina di Indoensia paling banyak adalah kasus penipuan dengan korban adalah warga Negara tiongkok sendiri.Puluhan WNA China dan Taiwan yang dibekuk petugas Polda Metro Jaya menyewa beberapa tower telekomunikasi untuk memudahkan aksi penipuan. Direktur Reserse

Kriminal Umum Polda Metro Jaya Kombes Pol Krisna Murti mengatakan, saat melakukan penggerebekan di rumah yang mereka tempati di Jalan Sekolah Duta V, Pondok Indah, Jakarta Selatan, petugas menemukan sejumlah alat elektronik yang dapat memudahkan para pelaku melakukan aksi penipuan. Menurut Krisna, pelaku memasang empat CCTV, dan membuat pemancar telekomunikasi di rumah.

"Komplotan ini juga menyewa menyewa beberapa tower telekomunikasi di Indonesia. Mereka ini melakukan penipuan melalui telepon dan internet," kata Krisna di Mapolda Metro Jaya, Minggu (24/5/2015). Krisna menuturkan, jaringan penipuan ini diduga menyewa tower telekomunikasi di wilayah Cilacap dan Sulawesi untuk melancarkan aksinya. "Sindikat ini sangat profesional karena mereka juga memasang tower kecil di atap rumah. Tower kecil ini mereka gunakan sebagai transmitter," tegas Krisna. Saat ini, perwakilan dari Kementerian Komunikasi dan Informasi tengah memeriksa peralatan yang digunakan sebagai tindak kejahatan cyber crime tersebut. Pada penggeledahan yang dilakukan pihak kepolisian, ditemukan uang tunai sebesar Rp365 juta dan puluhan paspor milik para pelaku. Sampai saat ini, pihak Polda Metro Jaya masih melakukan pengejaran terhadap jaringan lainnya yang diduga masih beroperasi di Jakarta.[34]

Selain itu pihak kepolisisan juga mengungkap kasus Tiga otak penipuan online yang melibatkan puluhan WNA China dan Taiwan dibekuk petugas Polda Metro Jaya. Ketiga dalang yakni, C, Hendri (40) dan Regen (32) merupakan warga Indonesia. Direskrimum Polda Metro Jaya Kombes Pol Krishna Murti menerangkan, Hendri dan Regen diringkus di area parkir Mangga Dua Square, Jakarta Pusat, usai petugas menangkap 21 WNA China dan Taiwan di Kemang, Jakarta Selatan. "Penangkapan Hendri dan Regen ini hasil pengembangan pengungkapan kasus penangkapan puluhan WNA China dan Taiwan di Pondok Indah, Pantai Indah Kapuk dan Cilandak beberapa waktu lalu

,"ungkap Krishna di Mapolda Metro Jaya, Senin (25/5/2015). Krishna menuturkan, C, Hendri dan Regen merupakan otak penipuan dari sindikat penipuan WNA China dan Taiwan ini. "Korban dari sindikat ini berada di China dan Taiwan. Kita juga sudah menangkap pelaku lain berinisial C yang merupakan ketua koordinator sindikat penipuan ini," ujarnya. C, lanjut Krishna, berperan menyediakan fasilitas sarana transaksi online. C

[34]Metro sindo news.com di akses 2 april 2016.

ini merupakan warga Jakarta yang berpura-pura tidak bisa bahasa Indonesia. "C belum kita ekspose karena masih dimintai keterangnya untuk pengembangan," terangnya.Kini, para pelaku terancam pasal berlapis. Mereka akan dikenakan Pasal 34 ayat (1) dan Pasal 28 ayat (1) jo Pasal 50 UU RI No 11/2008 tentang Informasi Transaksi Elektronik (ITE), Pasal 2 UU RI No 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Manusia, Pasal 3 UU RI No.21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Manusia dan Pasal 120 dan Pasal 124 a UU RI No.6/2011 tentang Keimigrasian.