
we preventcrime
public media of criminology
Dunia Maya,
Ancaman Nyata
Maret 2014
Desain Sampul : Sherlyna Rizki
GRATIS
EDISI
14
DEPARTEMEN KRIMINOLOGI
FISIP UI
HIMPUNAN MAHASISWA KRIMINOLOGI

wepreventcrime
public media of criminology

TIM REDAKSI

Redaksi :
Gedung Nusantara 1
Fakultas Ilmu Sosial Ilmu Politik
Universitas Indonesia
No. Tlpn 085719443917
Kritik dan saran dapat dikirimkan ke email *wepreventcrime*.

www.wepreventcrime.org
wepreventcrime@yahoo.co.id
@wepreventcrime

EDITORIAL

Seiring berzamannya sang kala, tuntutan akan perkembangan selalu membayangi manusia. Penemuan demi penemuan bermunculan sebagai jawaban atas kebutuhan, yang juga berkembang atau bahkan berubah. Arus kemajuan teknologi semakin deras dengan dimotori perkembangan pola pikir si empunya kebutuhan: manusia. Namun kehadiran dan kemajuan teknologi pun seakan menjadi ular berkepala dua, karena juga ada satu sisi manusia yang terus berkembang dan membutuhkannya, bahkan juga berkontribusi dalam mengembangkannya, yakni para pelaku kejahatan.

wepreventcrime mencoba membahas *cyber crime* sebagai salah satu bentuk dan dampak evolusi manusia. Perubahan zaman dan pola hidup manusia manusia tentunya juga mengubah kesempatan partisipasi dalam kejahatan, baik sebagai pelaku atau pun korban. Kehadiran dan kemajuan teknologi pun di satu sisi menciptakan kesempatan, celah, modus, dan berbagai elemen penting lainnya dalam kejahatan.

Redaksi

KONTEN

QUOTE'S

"Don't believe anything you read on the net. Except this. Well, including this, I suppose."
-Douglas Adams-

Jejaring Sosial dan Kejahatan Cyber

"The Internet is like a vault
with a screen door on the back.
I don't need jackhammers and atom bombs to
get in when I can walk in through the door."

William R. Cheswick

Agung Setya Sultani, mahasiswa Kriminologi 2011

Kata-kata diatas diucapkan oleh salah satu pencipta *Firewall* pertama di dunia sebagai penggambaran betapa rentannya sistem informasi dari celah-celah yang dapat dieksploitasi oleh pelaku kejahatan. Kejahatan di dunia digital terus berkembang semenjak pengunaan komputer komersil pertama hingga era jejaring sosial seperti sekarang ini, jika kita melihat kembali sejarah, pada awalnya komputer masih berbentuk "*mainframe*" dan merupakan aset yang sangat mewah bagi sebuah perusahaan dengan penggunaan yang sangat terbatas, kemunculan komputer menjadi sebuah inovasi bagi pelaku kejahatan tertentu dengan menyediakan wadah baru untuk melakukan kejahatan, ketika itu pelaku kejahatan yang muncul merupakan individu dengan akses menggunakan komputer. Pada tahun 1990, ketika komputer personal berkembang dan Internet mulai menghubungkan semua komputer yang ada kedalam jaringannya, secara sadar atau tidak, hal ini berarti memunculkan jutaan "suitable target" bagi pelaku kejahatan cyber, dan pada masa ini muncul aktifitas dalam bentuk "baru" pada kejahatan cyber, dibantu dengan perkembangan malware, aktifitas pelaku kejahatan cyber dalam melakukan aksinya menjadi lebih mudah.

Ketika kita bertanya, apa masalahnya jika kita menggunakan internet untuk kepentingan pribadi seperti jejaring sosial? Ketika itu pula kita telah menjadikan diri kita sebagai salah satu "vulnerable target" dari kejahatan cyber. Kejahatan cyber telah terjadi pada diri kita cukup lama tanpa kita sadari, bayangkan ketika kotak surat dirumah kita dipenuhi oleh surat-surat palsu berisi penipuan dan iklan yang bahkan kita tidak ketahui siapa pengirimnya, dan bayangkan ketika kita berada didalam satu ruang publik namun kemudian ada seseorang yang terus menatap dan memperhatikan kita, setiap hari dan setiap saat dia mampu. Di era jejaring sosial, aktifitas-aktifitas tersebut terjadi setiap saat, ketika kita membuka e-mail dan menemukan ratusan surat yang kita tidak inginkan, mungkin kita menganggap hal tersebut adalah sesuatu yang biasa/sepele, namun kenyataannya kita telah menjadi korban Spamming dan Scamming. dan disaat kita membagikan 140 karakter informasi tentang diri kita, keluarga kita, pengalaman kita, event yang sedang kita lalui, serta luapan rasa gembira dan marah dalam jejaring sosial, mungkin pada awalnya kita merasa sendiri atau mungkin kita menganggap bahwa informasi tersebut hanya akan dibaca oleh orang yang kita kenal, namun pada kenyataannya kita ditatap oleh ratusan atau bahkan ribuan pasang mata, yang pada dunia nyata mungkin memiliki hubungan yang tidak baik dengan diri kita.

Kondisi ini merupakan ancaman yang serius bagi keamanan individu, selain jejaring sosial memberikan kenyamanan bagi kita untuk berinteraksi dengan orang yang kita kenal, jejaring sosial juga memberikan sarana yang sangat strategis bagi pelaku kejahatan cyber untuk melakukan aksinya. Kebanyakan dari kita menganggap bahwa jejaring sosial merupakan sebuah ruang pribadi yang dapat dijadikan ajang untuk meluapkan kebebasan berpendapat tanpa adanya tanggung jawab, tidak dapat kita pungkiri bahwa disaat menggunakan jejaring sosial kita pernah melontarkan penghinaan atau pencemaran nama baik pada orang lain, menyebarkan informasi rahasia namun seringkali kebanyakan dari kita lupa jika kita tidak sendiri dalam jejaring sosial.

Jejaring sosial pada dasarnya merupakan 'realita virtual' dimana individu-individu yang berinteraksi didalamnya memiliki bentuk dalam dunia nyata, namun realita yang terbentuk didalam ruang virtual berbeda dengan realita yang ada pada dunia nyata, siapapun dapat menjadi apapun didalam internet dan karakteristik seseorang dapat berbeda 180 derajat ketika berada didalam dunia virtual, oleh karena itu kita harus mencoba membangun kesadaran untuk menyaring apa yang kita katakan dan apa yang kita bagikan, karena apapun yang kita katakan dan bagikan di internet, tidak akan pernah hilang.

Agung Setya Sultani
Kriminologi 2011

Kerangka Dasar Cyber Crime

Sistem informasi saat ini merupakan sumber daya dan mempunyai peranan yang sangat penting dalam keberlangsungan organisasi. Sistem informasi dipandang mempunyai nilai strategis yang dapat membuka peluang-peluang baru, serta sangat berperan sebagai daya kompetensi dan kompetisi. Pada setiap pengembangan dan implementasi sistem informasi sering dikaitkan dengan kenyamanan, kemudahan, efisiensi dan keuntungan yang dijanjikan atau ditawarkan.

Seiring dengan keuntungan yang ditawarkan, disadari bahwa sistem informasi juga semakin rentan akan potensi ancaman (threats). Hal ini dapat dilihat dengan mengacu pada tulisan Ward dan Peppard (2002) tentang perkembangan sistem informasi dan juga tulisan McGee (2001) tentang perkembangan dan dampak kejahatan komputer. Ward dan Peppard membagi perkembangan sistem informasi berdasar 5 (lima) aspek yaitu teknologi, operasional, pengembangan, alasan penggunaan teknologi dan karakteristik sistem. Berdasarkan aspek-aspek tersebut Ward dan Peppard menyatakan terdapat 3 (tiga) era perkembangan sistem informasi, yaitu era data processing (DP) pada tahun 1960-an, management information systems (MIS) di tahun 1970-an dan strategic information systems (SIS) sejak tahun 1980-an. Pada era SIS ini, menurut McGee generasi pertama kejahatan terhadap sistem informasi mulai muncul, berkembang dan semakin serius dari sisi jenis, frekuensi maupun dampak yang ditimbulkan.

Strebe (2004) menuliskan hal serupa dalam bukunya, ketika mendeskripsikan sejarah keamanan komputer. Bahkan menurut Strebe, ditegaskan kejahatan terhadap sistem komputer sudah dimulai pada saat kemunculan komputer itu sendiri dan semakin dipermudah pada pertengahan tahun 1975-an, ketika penggunaan microcomputer dan modem semakin meluas. Bahkan Strebe menuliskan bahwa penayangan film War Games pada pertengahan tahun 1980-an, dipandang turut berperan sebagai pemicu dilakukannya kejahatan dan menyuburkan budaya hacker.

Strebe juga menekankan bahwa sistem komputer merupakan suatu lingkungan yang tercipta dalam kondisi tidak aman dikarenakan beberapa hal, antara lain yaitu :

1) *Security is an annoyance*. Suatu situasi yang aman hanya dapat terwujud jika semua individu yang terkait dalam sistem informasi selalu belajar dan memahami faktor-faktor yang dapat menyebabkan kegagalan sistem. Hal ini tentu saja merepotkan sehingga tidak semua individu yang terkait mau untuk melakukannya.

2) *Features are rushed to market.* Vendor lebih mengkonsentrasikan diri pada upaya penambahan feature dari produk-produk teknologi informasinya dengan alasan meningkatkan kegunaan dari produknya. Aspek keamanan tidak menjadi perhatian atau pertimbangan yang serius.

3) *Vendors who spend time on security are eclipsed by the competition.* Ini terkait dengan keunikan dari pasar teknologi informasi. Konsumen teknologi informasi lebih tertarik untuk menggunakan produk terbaru, meskipun belum terbukti keamanannya. Produk teknologi informasi seperti itu cenderung akan menjadi rebutan konsumen dan kemudian menjadi standar.

4) *Computers and software evolve very quickly.* Termasuk teknologi jaringan. Dalam konteks tertentu produk teknologi informasi tersebut memang tidak dirancang dengan memperhatikan aspek keamanan. Namun kesemuanya dapat diterima oleh masyarakat, banyak digunakan dan menjadi populer.

5) *Programmers can't accurately predict flaws.* Perangkat lunak yang dikembangkan dan kemudian di-deploy dalam lingkungan yang berbeda. Ketika di-deploy perangkat lunak berada dalam suatu lingkungan, dimana terdapat jutaan pelaku kejahatan yang telah siap melakukan serangan.

6) *There is little diversity in the software market.* Khususnya sistem operasi, hanya terdapat Windows atau Unix. Sehingga pelaku kejahatan dapat lebih fokus dalam dalam memilih sasaran kejahatannya.

7) *Vendors are not motivated to reveal potential flaws*. Dengan berbagai alasan. Sementara di sisi lain hacker dengan tekun bersama-sama mencari, mendiskusikan dan merancang serangan terhadap kelemahan tersebut.

8) *Patches are not widely deployed and can cause problems when they are installed.* Tidak semua pengguna sistem informasi mau melakukan patch up-date kecuali telah menjadi korban. Di sisi lain sering terjadi ketika melakukan patch up-date yang muncul kemudian adalah bug atau menurunnya performa sistem.

Dengan adanya kesadaran bahwa sistem informasi merupakan lingkungan yang tidak aman, maka pengelolaan sistem informasi juga harus diimbangi dengan perhatian yang serius terhadap keamanan sistem informasi (information system security). Keamanan sistem informasi menjadi salah satu bagian

yang penting dalam melakukan pengelolaan sistem informasi. Prinsip-prinsip kerahasiaan, integritas dan ketersediaan informasi *(confidentiality, integrity and availability - CIA*) menjadi taruhan dalam kebijakan keamanan sistem informasi yang diambil. Prosedur dan mekanisme keamanan harus mampu menjamin sistem informasi dapat terlindungi dari potensi ancaman yang mungkin timbul.

Dari banyak data hasil survey tahunan *(e-Crime Watch Survey, U.S Secret Service dan CERT)* secara umum terlihat, *hackers* merupakan ancaman terbesar bagi keamanan sistem informasi. Para *stakeholders* seperti pegawai aktif dalam organisasi *(current employees)* bahkan hingga konsumen atau rekanan usaha juga dianggap atau dipersepsikan sebagai potensi ancaman terhadap sistem informasi. Ironisnya, dalam survey tersebut juga terungkap bahwa masih terdapat responden yang tidak tahu atau belum dapat mengidentifikasi ancaman terhadap sistem informasinya.

Keamanan sistem informasi, mensyaratkan untuk mengedepankan upaya-upaya yang bersifat pencegahan *(prevention)* terhadap potensi ancaman yang mungkin timbul, dibandingkan upaya-upaya pendeteksian kejahatan terhadap sistem informasi, penuntutan terhadap pelaku kejahatan atau pun upaya pemulihan kerusakan sistem informasi. Pencegahan menjadi penting karena pencegahan dapat menghindarkan pengelola atau pemilik sistem informasi dari timbulnya kejahatan *(computer related crime)* yang lebih lanjut, kerugian yang lebih besar dan, seperti yang ditegaskan oleh Ward dan Peppard, upaya atau biaya yang besar dalam upaya melakukan deteksi, menempuh proses hukum dan *recovery* terhadap sistem informasi yang rusak.

Sayangnya belum banyak organisasi yang mampu memenuhi atau mencapai suatu kendali yang efektif di dalam upaya pencegahan kejahatan terhadap sistem informasinya. Hal ini kemudian berdampak bukan saja kepada teraktualisasinya ancaman terhadap sistem informasi, tetapi juga berulangnya kejahatan serupa terhadap korban yang sama (repeating victimization). Potensi ancaman yang teraktualisasi memunculkan variasi bentuk-bentuk kejahatan terhadap sistem informasi seperti virus komputer, denial of service, SPAM, unauthorized access, phising dan lain sebagainya.

Dampak

Jumlah kerugian yang muncul akibat kejahatan terhadap sistem informasi cenderung untuk meningkat setiap tahunnya, bahkan yang dapat dihitung atau dikuantifisir akibat kejahatan terhadap sistem informasi menunjukkan angka yang tidak sedikit, dan sering kali kerugian tersebut sulit atau tidak dapat dihitung. Ketika kejahatan terhadap sistem informasi terjadi, bukan hanya aspek tangible yang rusak, akan tetapi juga banyak aspek intangible dari sistem informasi yang ikut rusak tidak dapat dihitung.

COBIT® Security Baseline™ - An Information Security Survival Kit menegaskan pula kerugian sebagai dampak *security incident,* yaitu; 1) *Competitive disadvantage.* Bocornya suatu informasi tertentu sehingga pada akhirnya jatuh ke pihak pesaing sedikit banyak dinilai akan berpengaruh terhadap organisasi. Dalam hal ini menurut Albanese dan Sonnenreich dalam tulisannya, akan sangat berpengaruh khususnya organisasi yang bergerak di bidang *research and development, intelijen,* pemasaran atau pun produsen produk IT dan layanannya.; 2) *Direct business loss.* Hilangnya pendapatan dan keuntungan; 3) *Loss of public confidence or reputation.* 4) *Poor morale.* Bukan saja hilangnya moral dari para anggota organisasi tetapi juga motivasi. 5) *Fraud.* 6) *Wrong management decision.* 7) *Business disruption.* Sebagai dampak ketidaktersediaannya aplikasi atau layanan informasi. 8) Legal liability. Dampak secara legal, regulatory atau pun kewajiban bersifat kontraktual. 9) *Privacy loss.* 10) *Safety risk.* Dampak bagi kesehatan, keselamatan ataupun kehidupan stakeholeder.

Strategi Pencegahan Kejahatan

Satu prinsip umum tentang pencegahan kejahatan adalah bahwa bagaimana pun kejahatan tidak mungkin ditekan sampai pada titik 0 (nol) akan tetapi harus dapat diusahakan bahwa kejahatan yang terjadi dan dampaknya masih berada dalam batas-batas yang dapat ditolelir. Kurang diperhitungkannya pendekatan sosial sebagai bagian yang holistik dalam upaya pencegahan kejahatan terhadap sistem informasi menyebabkan upaya yang selama ini dilakukan jelas belum dapat menekan terjadinya kejahatan dan kerugian. Sehingga disadari perlu untuk memasukkan pendekatan sosial dalam upaya pencegahan kejahatan terhadap sistem informasi.

Satu pendekatan sosial tentang pencegahan kejahatan yang dapat digunakan adalah pendekatan pencegahan kejahatan situasional. Pendekatan ini pada dasarnya memfokuskan diri pada pelaku kejahatan dan konteks lingkungan tempat terjadinya kejahatan, berusaha untuk memperoleh gambaran akan terjadinya kejahatan, khususnya dari sudut pandang pelaku kejahatan. Menurut pendekatan ini, apabila deskripsi itu dapat diketahui maka dapat dibuat suatu strategi pencegahan terhadap kejahatan.

Pencegahan kejahatan yang perlu dilakukan menurut Adamski setidaknya dilakukan dengan 2 (dua) cara atau prinsip, yaitu; 1) Mengurangi kesempatan, dengan memberikan perhatian kepada basic controls, seperti misalnya *kriptografi, password authentication, dan firewalls.* 2) Meningkatkan resiko bagi pelaku kejahatan, misalnya dengan meningkatkan kemampuan aparat penegak hukum dalam menangani kejahatan atau menjalin kerja sama antar negara dalam menangani kasus kejahatan.

Kisnu Widagso

Cyber Crime Mengancam Kita

Middleton (2001) mengatakan perkembangan tekhnologi yang begitu pesat telah memunculkan suatu bentuk teknologi baru yang berbasis computerized crime, yang menandai lahirnya teknologi media komunikasi internet. Teknologi komunikasi ini menjadi begitu penting disamping kemampuannya menyediakan informasi secara universal tetapi juga dengan jaringan kerja yang begitu luas dan kemampuan akses yang cepat dengan jarak yang lebih luas melalui saluran-saluran alternatif, informasi ditransmisikan dan diproses. Internet sebagai media komunikasi mutakhir bisa dipahami sebagai bagian dari komunikasi massa yang tujuannya memberikan informasi seluas-luasnya kepada khalayak. Internet memungkinkan semua pihak saling berhubungan dan berinteraksi setiap saat. Internet menyajikan segala bentuk informasi yang komplit dan prulalistik (Golose, 2008:7)

Creeber, Glen & Royston (2009) menyatakan keberadaan dunia maya *(cyber space)* sebagai salah satu kemajuan teknologi dewasa ini membuat suatu pergeseran atau perubahan yang sangat cepat ke dalam kehidupan dunia yang tanpa batas *(borderless world)*. Berbagai informasi tidak hanya disajikan melalui hubungan jarak jauh dan tidak harus bertatap muka tetapi cukup dengan peralatan dan koneksi telekomunikasi. Internet sebagai salah satu hasil dari perkembangan teknologi dewasa ini tidak hanya berfungsi sebagai mesin pencari *(search engine)* namun juga menyajikan beberapa layanan yang diwujudkan dalam bentuk portal berita, blog hingga situs jejaring sosial.

Menurut Mech (2009), Internet bukan hanya alat komunikasi super canggih untuk mendapatkan, menyebarkan dan bertukar informasi dengan cepat, mudah, luas, multimedia dan multiformat, akan tetapi internet dapat digunakan sebagai alat kejahatan yang super-fungsi pula. Semakin banyak fasilitas yang ditawarkan di internet, semakin besar pula peran internet membantu aktifitas kita dan semakin lebar pula celah terbuka bagi oknum-oknum tertentu yang tidak bertanggungjawab untuk melakukan kejahatan melalui internet. Internet dalam hal ini dapat menjadi suatu alat yang dapat memunculkan hal yang dapat menyerang dan membahayakan (Mesch, 2009). *Cyber crime* atau kejahatan yang terjadi pada dunia internet pun muncul seiring dengan perkembangan teknologi. Salah satu kejahatan yang terjadi di Internet adalah *cyber victimization* yang merupakan *viktimisasi* lewat internet.

John Spiropoulos (1999) mengungkapkan bahwa *cybercrime* memiliki sifat efisien dan cepat serta sangat menyulitkan bagi pihak penyidik dalam melakukan penangkapan terhadap pelakunya.

Collin Barry C. menjelaskan istilah *cybercrime* sebagai berikut :

"*Term "cyber-crime" is young and created by combination of two words: cyber and crime. The term "cyber" means the cyber-space (terms "virtual space", "virtual world" are used more often in literature) and means (according to the definition in "New hacker vocabulary" by Eric S. Raymond) the informational space modeled through computer, in which defined types of objects or symbol images of information exist – the place where computer programs work and data is processed."*

Natalie D. Voos di dalam *"Crime on The Internet"* (1999) menguraikan beberapa jenis *Cybercrime* berdasarkan beberapa issu yang menjadi bahan studi atau penyelidikan pihak FBI dan *National White Collar Crime Center* sebagai berikut : *A) Computer network break-ins, B) Industrial espionage, C) Software piracy, D) Child pornography, E) E-mail bombings, F) Password sniffers, G) Spoofing, H) Credit card fraud.*

Cyber crime dan Indonesia

Banyak kasus *cyber crime* yang terjadi di Indonesia, Contohnya saja pada tahun 2009 hacker-hacker Indonesia yang menamakan dirinya IndonesianCoder Team dan ServiceIsDown melakukan *massdeface* (penyerangan) terhadap situs-situs Malaysia pada hari ulang tahun kemerdekaan Malaysia yang ke-52. Situs-situs yang diserang yaitu situs resmi Persatuan Guru-guru di Sarawak (stu.org.my), bagsmalaysia.com, globalmarine.com.my, mgpskuantan.edu.my dan puluhan situs lainnya yang menurut para hacker-hacker tersebut hal itu dilakukan untuk memberikan peringatak kepada Negara Malaysia agar tidak mengusik lagi kebudayaan Indonesia. Kemudian kasus *cybercrime* yang dilakukan oleh Yogyacarderlink dimana mereka telah meretas dan menyerang situs-situs milik pemerintah Indonesia seperti situs milik Departemen Pertanian, Departemen Kebudayaan dan Pariwisata, situs sejarah TNI bahkan situs milik presiden Mongolia. Yogyacarderlink selalu meninggalkan pesan *"We Can Do All You Can't Do"* dalam situs yang mereka retas dengan harapan adanya perbaikan kinerja para pejabat pemerintahan melalui peringatan awal dari mereka.

Ilustrasi Foto Hacker WPC/Andreas Meiki

Pada konteks Indonesia, ancaman *cyber crime* mengarah pada penerapan *E-Goverment. National Technology Officer Microsoft Indonesia,* Tony Seno Hartono mengungkapkan pentingnya perlindungan kejahatan dunia maya terhadap layanan internet di pemerintahan (E-Government) (Tempo.co 5/9/13). Biasanya yang sering terjadi adalah peretasan terhadap sistem E-Government. Dulu, penyerangan biasanya dilakukan lewat virus-virus malware-sekarang yang terjadi adalah pembobolan situs itu sendiri. Ini disinyalir karena beberapa hal, salah satu diantaranya adalah perancang program yang dipkerjakan secara outsource (alih daya). Bisa jadi, mereka yang telah keluar kembali berulah pada hasil ciptaan mereka. Seperti yang dijelaskan oleh Ketua Tim *Cyber Crime Investigation Course* Akademi Kepolisian Semarang, Komisaris Besar Polisi Winston Tommy Watuliu dalam Tempo.co 5/9/13, ia mengatakan terdapat tiga hal untuk meminimalisir kejahatan di dunia maya. Pertama, berasal dari pemiliki, yaitu pemerintah. Kedua adalah peran administrator yang sesuai dengan kriteria suatu instansi. Ketiga adalah kolaborasi yang baik antara penyidik dan administrator.

Berdasarkan motif kegiatannya *cybercrime* termasuk dalam Kejahatan yang murni merupakan tindak kriminal yang dilakukan karena motif kriminalitas. Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan *cybercrime* juga jenis kejahatan di internet yang masuk dalam wilayah "abu-abu", cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. *Cybercrime* juga sering dikaitkan dengan kejahatan lain seperti terorisme, stalking, pornografi, pedofilia dan jenis kejahatan apapun yang memanfaatkan media internet. Jadi, *cybercrime* tidak berdiri sendiri, melainkan menjadi sarana maupun pendukung keberadaan kejahatan lain yang tentunya tidak hanya dalam ruang lingkup lokal atau sempit tapi telah melebarkan sayapnya dalam ruang lingkup global.

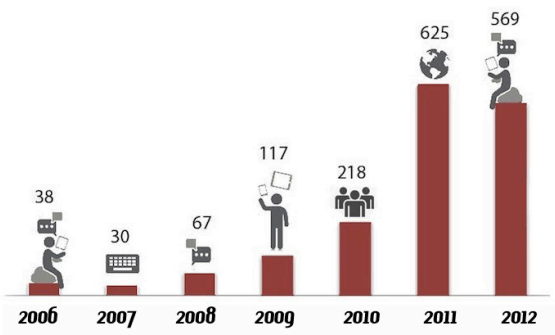
Ayu Permata, Kahfi Dirga Cahya

Kinerja Unit Polda Cyber Crime

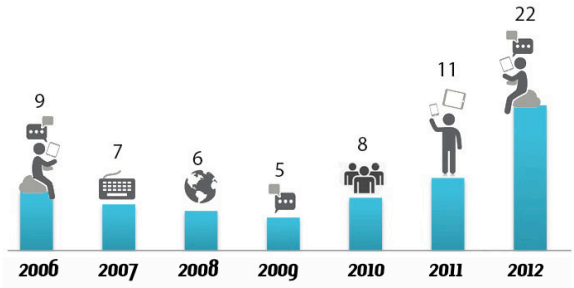
Perkembangan teknologi informasi yang demikian pesat belakangan ini selain memberi dampak positif juga menimbulkan dampak negatif. Teknologi-teknologi yang membantu kita mendapatkan informasi dengan lebih cepat dan mudah dapat dimanfaatkan oleh oknum-oknum tertentu untuk berbuat kejahatan. Kepolisian Republik Indonesia termasuk salah satu lembaga yang menyadari betapa berbahayanya perkembangan teknologi yang terjadi belakangan ini. Sejak tahun 2003, dibangun Divisi Kriminal Khusus Unit Cyber Crime Polda Metro Jaya yang berada di naungan Badan Reserse Kriminal Khusus. Divisi ini telah menangani begitu banyak kasus yang bervariasi modusnya, seperti penipuan sms, penipuan kartu kredit, pencemaran nama baik, dan lain-lain.

Pekerjaan divisi ini semakin bertambah banyak setiap tahunnya. Melalui data perkara yang didapat dari Divisi Kriminal Khusus Unit Cyber Crime Polda Metro Jaya, sejak tahun 2006 sampai tahun 2012 terjadi peningkatan kasus kejahatan siber yang cukup pesat. Dari tahun 2006 yang hanya masuk 38 kasus berkembang menjadi 569 kasus di tahun 2012 (Naik 1500%). Kejahatan siber paling banyak terjadi pada tahun 2011 dengan jumlah kejahatan 625 kasus. Hal ini wajar terjadi mengingat tren *smartphone* yang dimulai pada tahun ini. Namun masyarakat tampaknya tidak bisa sepenuhnya berharap kepada bagian Divisi Kriminal Khusus Unit Cyber Crime Polda Metro Jaya. Dilihat dari data yang didapatkan, kasus kejahatan siber yang telah tuntas dilimpahkan ke kejaksaan berbanding jauh dengan jumlah yang masuk. Hanya 8 dari 218 kasus tahun 2010, 11 dari 625 kasus tahun 2011, 22 dari 569 kasus tahun 2012 yang dilimpahkan ke kejaksaan.

Jumlah Kasus



Jumlah Kasus yang Dilimpahkan ke Pengadilan



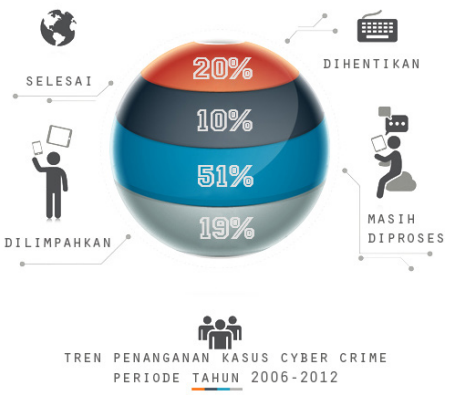
.Efektivitas kinerja kepolisian bisa dilihat dari selesai atau tidaknya penyelidikan yang dilakukan hingga berkasnya telah dirasa cukup untuk dilimpahkan ke kejaksaan. Apabila indikator ini yang dipakai maka dapat dikatakan bahwa kinerja Polda Metro Jaya dalam menangani kasus kejahatan siber masih rendah. Hanya pada tahun 2006 dan 2007 saja persentase kasus yang diselesaikan lebih dari 20%, yakni 23,68% dan 23,33%. Pada tahun 2011, persentase kasus yang dilimpahkan hanya sebesar 1,76% saja. Dari data statistik, persentase rata-rata kasus yang perkaranya selesai sampai dilimpahkan ke kejaksaan hanya 9,93%.

Pada tahun 2006, 2007, dan 2009, cukup banyak kasus yang dihentikan penyelidikannya. Sebanyak 52,63% kasus yang terjadi di tahun 2006 dihentikan penyelidikannya, begitu juga 30% kasus yang terjadi di tahun 2007 dan 26,5% kasus yang terjadi di tahun 2009. Alasan penghentian penyelidikan ini bisa bermacam-macam, seperti kekurangan bukti, habis masa penindakan, dan si pengadu mencabut laporan.

Pada tahun 2006 sampai 2009 hanya sedikit kasus yang dilimpahkan ke divisi kepolisian lain, yakni sebanyak 2 kasus saja. Pada empat tahun ini kejahatan-kejahatan yang masuk ke divisi ini belumlah terlalu bervariasi sehingga metode penyelesaiannya sama. Namun pada dua tahun terakhir pelimpahan kasus membengkak, yakni 240 kasus pada tahun 2011 dan 318 kasus pada tahun 2012. Eskalasi ini bisa disebabkan karena semakin banyaknya modus kejahatan komputer baru yang ditemukan sehingga penyelidikannya tumpang tindih dengan divisi lain di kepolisian. Contohnya kejahatan penipuan dengan menggunakan website, meski termasuk kejahatan siber, bisa dilimpahkan ke divisi kriminal umum.

Sisa kasus yang lain masih dalam tahap proses penyelidikan dan penyidikan. Namun karena proses tersebut berjalan terus-menerus hingga keputusan selanjutnya, kasus dari tahun-tahun yang sudah lewat masih ditangani sampai sekarang. Dengan demikian dari tahun 2006 sampai 2012 tunggakan kasus yang masih diproses mencapai 849 kasus (51.02%).

Melalui data yang diterima dari Divisi Kriminal Khusus Unit Cyber Crime Polda Metro Jaya kita bisa melihat persentase tren penanganan kasus kejahatan siber yang masuk dari tahun 2006-2012. Mayoritas tren penanganan kasus adalah masih dalam tahap pemrosesan hingga saat ini (51,02%). Sedangkan tren penanganan kasus kejahatan komputer dengan melimpahkan berkasnya ke kejaksaan merupakan minoritas, ditunjukkan dengan persentase 9,93%.



Dari data yang didapat di atas, tidak dapat langsung disimpulkan bahwa Divisi Kriminal Khusus Unit Cyber Crime Polda Metro Jaya tidak bekerja dengan baik. Ada beberapa faktor yang menyebabkan kejahatan siber ini tidak mudah ditangani. Yang pertama adalah kurangnya sumber daya manusia di divisi ini, yang hanya berjumlah sebanyak 43 orang padahal mereka bisa menangani hingga 100 kasus setiap tahunnya. Yang kedua adalah pengaduan kasus biasanya baru dilakukan setelah kasus itu lama berselang padahal jejak kasus kejahatan siber mudah sekali hilang.

Albert Wirya,

AKBP Silvester Simamora, SIK, Tim IT di Divisi Kriminal Khusus Unit Cyber Crime Polda Metro Jaya. WPC/Tyas W.

Investigasi Cyber Crime: Optimis Tanpa Henti

Seorang perwira Kepolisian Republik Indonesia yang bernama Silvester Simamora ini adalah salah satu anggota dari Tim IT di Divisi Kriminal Khusus Unit Cyber Crime Polda Metro Jaya. Sebelumnya dia ditempatkan di Cyber Crime Mabes POLRI selama 3 - 4 tahun dan baru-baru ini ditempatkan di Polda Metro Jaya pada divisi dan unit yang sama. Beliau merupakan lulusan dari akademi kepolisian (AKPOL), kemudian melanjutkan ke Perguruan Tinggi Ilmu Kepolisian (PTIK). Pada tahun 2003 ia lulus dari Perguruan Tinggi Ilmu Kepolisian (PTIK), dan ditempatkan di Mabes Polri Unit Cyber Crime. Sebelum ditempatkan di Polda Metro Jaya, Pak Sivester pernah menimba ilmu mengenai cyber crime selama 2 minggu di Korea Selatan. Pada akhirnya ditempatkan di Polda Metro Jaya.

Suara hujan yang sangat deras dan dinginnya *air conditioner* yang menyelimuti ruang rapat Unit Cyber Crime Polda Metro Jaya, tak kami rasakan. Kami tim *wepreventrime*, dengan semangat mendengarkan kisah beliau tentang motivasinya untuk mendalami dunia *cyber crime*. "Alasannya simple, kejahatan sekarang ini sudah banyak berpindah ke ranah *cyber crime* juga. Di dunia *cyber crime* sendiri, sebenarnya banyak *opportunity* yang tidak banyak orang lain sadari" ujarnya dengan santai namun penuh semangat dalam penyampaiannya.

Di sore yang diselimuti oleh cuaca yang masih gelap karena berhentinya hujan, Pak Silvester masih menceritakan tentang pengalaman-pengalaman yang ia alami ketika melakukan tugas-tugasnya dalam ranah *cyber crime*. Selama ia bertugas di unit *cyber crime*, ada tiga kasus yang sampai sekarang menjadi kenangan yang tidak terlupakan. Ia menuturkan semua emosi yang ada di dalam dirinya terluapkan ke dalam tiga kasus itu. "Ada tiga kasus yang *gak* bisa saya lupakan. Semua emosi saya pun keluar untuk menangani kasus-kasus ini semasa saya bekerja di Cyber Crime Mabes Polri. Kasus-kasus yang saya tangani saat itu, termasuk ke dalam penipuan dunia

maya. Akan tetapi, korban-korbannya tersebar di tiga negara yaitu Singapura, Swedia, dan Colorado dan pelakunya semua berasal dari Indonesia. oleh sebab kejahatan

Cyber Crime yang ditangani oleh Mabes Polri sifatnya lintas negara atau kerap dikenal sebagai kejahatan *transnasional.* Biasanya bentuk pelaporannya melalui agen-agen penghubung yang bekerja sama dengan Mabes Polri seperti FBI, Interpol, dan lainnya. "Jadi, *pas* saya menangani kasus penipuan yang ada di Colorado. Yang melapor ke pihak Mabes Polri saat itu orang dari FBI. Jadinya saya beserta rekan-rekan saya harus berangkat ke Colorado untuk menemui korbannya juga," dengan semangat iya menuturkan kisahnya.

Di tengah kesibukannya yang padat, tentu ada suka - duka yang telah ia alami. Seperti kurangnya sumber daya manusia dalam mengurusi kasus *cyber crime* karena hanya terdapat 50 orang di unit *cyber crime* sehingga harus bekerja secara ekstra untuk menghadapi kasus yang terus berdatangan. Sedangkan *Cyber Crime* Polda Metro Jaya membawahi banyak polres dan polsek yang ada di wilayah DKI Jakarta ini. Tidak sebanding memang dengan jumlah personil yang ada di kantor. Ia pun sangat ingin menggunakan tenaga-tenaga ahli seperti hacker-hacker yang masih ada di luar dari Cyber Crime Polda Metro Jaya.

"Di dunia cyber crime sendiri, sebenarnya banyak opportunity yang tidak banyak orang lain sadari "

Menurutnya tentu akan mempermudah penyelesaian kasus-kasus yang ditangani. "Saya ingin sekali untuk merekrut orang-orang seperti *hacker-hacker* ke dalam unit *cyber crime.* Selain untuk membantu kami dalam melaksanakan tugas juga, saya ingin memberikan sebuah bentuk apresiasi juga kepada mereka. Karena bakat-bakat yang seperti ini sangat sayang kalau tidak di manfaatkan. Daripada kita biarkan mereka ada di penjara atau kita lepaskan begitu aja. Lebih baik kita manfaatkan mereka sebagai rasa apresiasi kita kepada mereka. Namun sekarang ini saya bukan sebagai *decision maker*" ujarnya sambil bercanda dan penuh semangat.

Ia juga menuturkan bahwa kesulitan yang anggota Polri alami ini karena belum terintegrasinya data-data dari penduduk Indonesia, terutama di wilayah DKI Jakarta. "Sebenarnya sulit juga bagi kami ketika data-data penduduk masih belum terintegrasikan. Karena ini akan menghambat kinerja kami juga. Coba kita lihat seperti Filipina, disana sekarang sudah terintegrasi semua data-data yang berkaitan dengan kependudukan. Jadi, mereka lebih gampang untuk melakukan proses pelacakan dan yang lainnya" ujarnya sambil menghela nafas dalam-dalam seakan-akan berat sekali ketika dihirup.

Ia juga menuturkan tentang bagaimana dilemanya ketika menangani kasus yang memang benar-benar dapat meluapkan emosinya. Terkadang dari laporan-laporan yang masuk terdapat kasus penipuan yang ia ingin langsung selesaikan. Karena selain ada rasa iba dan juga kasihan terhadap korbannya, ia juga ingin segera menyelesaikan ke kasus selanjutnya. "Sebenarnya kalau kami menerima laporan yang korbannya kehilangan di bawah 2 juta, kami ingin sekali menyelesaikan dengan memberi uang ganti saja. Selain iba, kami juga ingin langsung menyelesaikan ke kasus selanjutnya".

Selain itu juga pengorbanan yang ia kerahkan sebagai bentuk dedikasinya terhadap negara tidaklah kecil. Karena ia harus masuk kerja pada jam 7 pagi dan kerja hingga waktu yang tidak ditentukan. Tergantung berapa banyak laporan dari masyarakat yang masuk terkait dengan *cyber crime*. "Kita kerja dari jam 7 pagi. Terkadang juga harus lembur karena jumlah laporan yang masuk pun banyak juga. Bahkan ketika weekend pun saya harus masuk kerja. Misalkan ketika saya sedang menghabiskan waktu dengan keluarga, saya mendapat panggilan dari atasan untuk masuk" tuturnya ketika kami wawancarai.

Tetapi karena Pak Silvester merasa tertantang dan tertarik dengan bidang *cyber crime* maka beliau pun dengan senang mengerjakannya. Di ujung pembicaraan, beliau pun yakin bahwa minat orang-orang terhadap *cyber crime* beberapa tahun ke depannya akan meningkat dan menjadi prospek yang diminati. "*Ya…* Kita lihat 10 tahun ke depan saja.

Pasti bidang *cyber crime* ini akan menjadi menarik sekali untuk dipelajari. Pada saat itu juga saya sudah menguasai bidang ini tentunya. Bagi saya *cyber crime* ini penting dikuasai dari sekarang karena banyak kejahatan yang sudah pindah ke ranah ini" tuturnya sambil mengakhiri wawancara kami.

Cyber Crime: Bukan Tidak Ada Penyelesaiannya

Cyber crime, atau kejahatan siber, merupakan tindak kriminal yang sangat dekat di kehidupan kita sebagai manusia berteknologi maju. Sisi negatif ini sudah diwaspadai oleh banyak orang, namun tetap saja terjadi. Sebenarnya, ada apa di balik penanganan *cyber crime* yang masih belum awam di mata masyarakat?

Apa itu *cyber crime*?

"Mengenai pengertian *cyber crime*—itu kembali pada masalah media. Kejahatannya sama saja seperti yang dirumuskan di KUHP, namun medianya yang membuat itu dikategorikan sebagai *cyber crime*," jelas AKP Slamet selaku anggota tim penyidik Subdirektorat (Subdit) IV Polda Metro Jaya, yang bertanggung jawab pada bidang cyber crime. Sejak berdiri pada tahun 2003, Subdit IV telah menangani ribuan kasus cyber crime. Di bawah naungan Reserse Kriminal Khusus Polda Metro Jaya, Subdit IV memiliki markas yang dikenal dengan nama *Cyber Crime Investigation Satellite Office*.

Penipuan dalam bentuk jual-beli secara online, pesan singkat, dan lain-lain masih menjadi pilihan yang efektif untuk memperoleh keuntungan. Sayangnya, proses kerja pengaduan korban kejahatan ini masih belum banyak diketahui. Sehingga dapat dikatakan, *cyber crime* merupakan 'jalan aman' melakukan tindak kriminal.

Semenjak awal berdirinya pada tahun 2003, *cyber crime* yang ditangani sudah beragam. Misalnya pada tahun 2003 sampai 2005, *cyber crime* sangat sedikit terjadi karena perkembangan teknologi yang belum pesat. Angka mulai meningkat di tahun 2005, melalui maraknya penipuan dengan media pesan singkat. Menurut AKP Slamet, *cyber crime* menggunakan pesan singkat sebagai medianya sampai kini masih menjadi bentuk yang paling dominan. Biasanya, modus yang digunakan adalah meminta korban untuk melakukan pengiriman sejumlah uang sebagai syarat mendapatkan hadiah.

Bagaimana proses penyelesaiannya?

Dalam menangani *cyber crime*, proses penyelidikan dan penyidikannya tidak jauh berbeda dengan kejahatan umum. Kompol Khaerudin—anggota penyidik Subdit IV—menjelaskan bahwa proses pengusutan cyber crime dimulai dari analisa kasus; apakah kasus tersebut termasuk ke dalam ranah *cyber crime*. Apabila iya, maka kasus akan diproses lengkap dengan surat penyidikan, dan dilanjutkan pencarian bukti untuk mengungkap permasalahan.

43 anggota tim penyidik dan tim IT Subdit IV dibagi menjadi tiga unit. Pemakaian KUHP masih merupakan hal yang penting dalam penanganan *cyber crime*. "Walaupun Undang-undang Informasi dan Transaksi Elektronik (UU ITE) sudah ada pada tahun 2008, KUHP masih paling dominan dipakai untuk memberikan dakwaan kepada pelaku. Karena sekali lagi, kejahatan ini hanya berbeda pada medianya saja," tambah Kompol Khaerudin.

Suasana Ruang Kerja Divisi Cyber Crime Polda WPC/Tyas W.

Selain tim penyidik, penanganan *cyber crime* juga bekerja sama dengan tim IT yang telah dilatih khusus. Tim penyidik hanya mengambil bagian pada penyidikan di lapangan, dan pembuat keputusan mengenai pasal atau hukum apa yang dilanggar. Sementara, tim IT merupakan tim pendukung penyidik, dan bekerja di balik layar. Tim IT berusaha menemukan bukti kejahatan yang sulit dilacak. Sering kali, bukti kejahatan yang sulit dilacak itu berupa data yang perlu *di-track*.

Masalah ketika menyelesaikan masalah

Dengan demikian, apa yang membuat tingkat *cyber crime* masih tinggi? Menurut Kompol Khaerudin, kewaspadaan dari para korban yang masih kurang serta tidak adanya pengetahuan yang baik mengenai *cyber crime* merupakan penyebab utama mengapa banyak individu yang berpotensi menjadi korban

Selain itu, dari sisi pihak Subdit IV sendiri, kurangnya sumber daya manusia dan biaya operasional yang kadang sangat tidak seimbang dibanding jumlah kasus yang harus ditangani merupakan masalah yang menghambat mereka untuk menuntaskan masalah *cyber crime*. "Walau pun kantor sudah cukup baik, terutama alat-alat yang digunakan tim IT, tapi tetap saja kurangnya sumber daya manusia dan dana yang kadang tidak cukup untuk melakukan penyidikan menjadi hambatan utama buat kami (Subdit IV)," tutur AKP Slamet.

Kerja sama antara korban dan aparat merupakan hal yang penting untuk mengatasi *cyber crime*. Korban harus turut bertanggung jawab atas dirinya sendiri, dan aparat diharap dapat membantu secara maksimal. Bila dilakukan, harapan untuk menurunkan tingkat *cyber crime* bisa tidak hanya sebatas menjadi wacana saja nantinya.

Tua Maratur Naibaho, Miranda Olga Viola

Tips Aman Berbelanja Online

Terdapat berbagai macam alasan mengapa individu lebih suka berbelanja online; lebih mudah untuk memilih dan mengakses barang yang ditawarkan, tidak memakan banyak waktu dan tenaga, variasi pilihan barang banyak, dan lain-lain. Namun, bukan berarti berbelanja online tidak memiliki kelemahan; risiko yang menyertai karena pembeli dan penjual bersifat anonym, minimnya interaksi langsung, absennya peraturan atau keamanan yang diilibatkan, dan sebagainya. Selain itu, pada transaksi jual-beli online, konsumen lebih rentan untuk menjadi korban penipuan. Tim wepreventcrime memiliki beberapa tips untuk menghindari penipuan jual-beli online, yaitu sebagai berikut:

1. Pilihlah situs jual-beli online yang terpercaya. Kaskus dan Toko Bagus adalah beberapa diantaranya. Faktor keamanan konsumen merupakan salah satu hal yang menjadi perhatian khusus dari situs tersebut. Untuk mengetahui terpercaya atau tidaknya situs jual-beli online, anda dapat meminta rekomendasi pada rekan anda yang telah memiliki pengalaman melakukan pembelian barang secara online.

2. Pada situs jual beli online, biasanya terdapat panduan mengenai beberapa tips bagi konsumen untuk melakukan transaksi yang aman dan terhindar dari penipuan. Hal tersebut bertujuan untuk mengedukasi konsumen agar dapat mengidentifikasi dan mengevaluasi penipuan. Oleh karena itu, sebelum melakukan transaksi, bacalah panduan tersebut.

3. Sebelum melakukan transaksi atau membuat kesepakatan, ada baiknya anda memastikan bahwa penjual tersebut telah direkomendasikan oleh situs terkait. Seperti di Toko Bagus, konsumen direkomendasikan untuk membeli barang pada verified member, karena data dan identitas penjual telah diverifikasi dan ia telah melakukan transaksi jual-beli yang benar.

4. Gunakan akal sehat dalam memilih penjual dan barang yang kita minanati. Jangan mudah tergiur dengan harga barang yang murah, diskon yang besar, ataupun jangan memilih barang BM (black market). Bila anda mudah tergoda oleh produk yang ditawarkan, kewaspadaan anda terhadap keamanan dalam bertransaksi secara online akan menurun dan rentan menjadi korban penipuan.

5. Anda dapat melihat baik atau buruknya testimoni konsumen yang sebelumnya pernah melakukan transaksi barang pada penjual, gunakan sebagai indikator terpercaya atau tidaknya penjual tersebut. Periksa juga situs asli penjual (bila ada) dan interaksi penjual dengan konsumen-konsumen sebelumnya serta tanggal terakhir situs beroperasi.

6. COD (Cash on Delivery) adalah model transaksi jual-beli online yang paling aman karena dapat menghindarkan anda dari kerugian dan penipuan. Jangan pernah mentransfer uang jika barang yang anda inginkan belum diterima, baik itu untuk uang muka ataupun pembayaran pajak dan lain-lain. Saat COD berlangsung, anda dapat membatalkan transaksi jika barang tersebut tidak sesuai dengan apa yang anda ekspektasikan. Lakukan transaksi COD di tempat yang aman, atau ajak rekan anda untuk menghindari hal-hal yang tidak diinginkan.

7. Biasanya, situs jual-beli online menyediakan moderator yang dapat anda tanyakan terkait beberapa informasi penting yang dibutuhkan. Apabila anda ragu atau kejanggalan terhadap penjual dan transaksi yang sedang anda lakukan, anda dapat menanyakan moderator mengenai kredibilitas penjual tersebut.

Nabila Riyas Putri, Yanuar Permadi

Sekedar Kata Tentang Era Informatika

Ruang Kerja Divisi Cyber Crime Polda WPC/Tyas W.

Perkembangan teknologi informasi dan komunikasi satu decade kebelakang telah banyak membawa perubahan bagi kehidupan kita, manusia modern. Hilangnya batasan jarak ruang dan waktu menjadi ciri utama dari perubahan ini. Kemudahan dan perubahan yang terjadi, seperti pada berbagai aspek kehidupan lainnya tentu memiliki "sisi lain" seperti pedang bermata dua.

Sederet panjang dampak positif yang dibawa oleh perubahan dengan mudah kita sadari. Sayangnya, semudah itu pula kita menyadari dampak negatif yang dibawa oleh perubahan tersebut.

Era digital, kata orang – orang, berpengaruh pula pada digitalisasi berbagai material berharga bagi kehidupan manusia. Adanya email, *e-trading,e-money* dan berbagai material berharga digital lainnya memicu pula perubahan bentuk ancaman dan kejahatan terhadap material tersebut.

Hacking, spamming, carding menjadi beberapa bentuk kejahatan modern yang lahir sebagai efek perkembangan teknologi informasi dan komunikasi.

Ironisnya, masih banyak dari kita yang secara sadar atau tidak memapar diri kita kepada resiko menjadi korban kejahatan secara digital. Kehadiran jejaring sosial seperti *facebook* lah yang jadi biang keroknya. Tak hanya material digital berharga, namun juga keselamatan fisik dan harta benda kita menjadi taruhannya.

Sikap acuh dan kecenderungan terlalu membuka diri di dunia digital seringkali membuat kita lengah dan berakhir pada kerugian yang menimpa kita, memang harus diakui, dunia digital merupakan tempat bersosialisasi dan berinteraksi pula, tetapi tak berarti kita menjadi lengah dan ceroboh dalam prosesnya.

Tak dapat dipungkiri memang, keselamatan dan keamanan kita sebagai manusia tak sepenuhnya hanya jadi beban pribadi saja. Sebagai warga Negara, tentunya pemerintah memiliki kewajian pula dalam melakukan perlindungan terhadap warga negaranya. Salah satunya dengan memberikan kepastian hukum.

Bukan hal yang baru ketika terjadi kerancuan dalam penindakan hokum terhadap suatu bentuk kejahatan, begitu pula dalam penegakan hokum terhadap *cyber crime* yang masih belum mampu memberikan perlindungan terhadap segala bentuk kegiatan virtual.

Kenyataan ini haruslah menjadi perhatian kita semua, tak hanya pemerintah semata. Tetapi kebanyakan dari kita yang sangat memanfaatkan perkembangan teknologi digital.

Meningkatkan kewaspadaan dan membatasi informasi diri yang sekiranya dapat membahayakan diri kita mutlak wajib dilakukan dalam era digital ini.

Harris Kristanto

Kebingungan yang Membingungkan

Dalam dunia internet, bisa saja yang 'bodoh' akan menjadi 'cerdik', dan yang 'pintar' akan 'dibodohi'. Dalam dunia internet, akan terdapat ambiguitas antara mana yang 'baik' dan mana yang 'jahat'. Jangan bingung, kalau anda bingung ya pegangan saja. #lawas

Kemajuan teknologi informasi yang sudah maju kini membuat berbagai hal menjadi lebih efisien, termasuk dalam pencarian *'entertainment'*, berbagai macam pengetahuan yang kita butuhkan, atau lain-lainnya. Langkah efisien tersebut adalah dengan menjelajahi dunia internet. Hal yang anda perlu lakukan hanyalah dengan membuka *search engine Google*, dan cari apa yang anda inginkan. Tidak heran bila banyak orang awam yang bercanda bahwa *Google* adalah Tuhan, karena merupakan sumber dari segala pengetahuan. Masih banyak para gombal-ers yang merayu orang lain dengan kalimat "kamu itu seperti *Google,* segala yang aku cari bisa ditemukan dalam diri kamu" *#eaa* –meskipun dalam kasus ini, harusnya gombalan yang digunakan bisa lebih *up-to-date*-.

Tapi, di sisi lain, Jika saya menjadi *Google,* saya akan merasa sedih. Banyak mahasiswa yang menggantungkan pengerjaan tugasnya pada *Google*, baik sebagai mesin pencari website terkait, maupun yang digunakan untuk *copy-paste* terjemahan tugas literatur asing dengan menggunakan *Google Translate* (ayo ngaku aja lah…). Namun, nama *Google* tidak pernah tertulis dalam Skripsi pada bagian Ucapan Terima Kasih seseorang. Apakah pernah ada yang menuliskan "*Thanks to Google*, tanpamu aku hampa, nestapa, dan bukan siapa-siapa. Aku dedikasikan titel sarjana ini untukmu" di Skripsi? Ibarat kata, namanya disebut-sebut saat lagi kesusahan, dijadikan teman curhat dan meminta pertolongan disaat membutuhkan, tapi disaat sedang berbahagia bersama orang lain akan dilupakan. Sakit, perih, miris.

Saya merupakan orang yang sering meluangkan waktu untuk browsing, meskipun itu miris karena membuat saya menjadi anti-sosial dan itu merupakan hal buruk. Entah mengapa saya sangat menyukai browsing, mungkin karena menurut saya dunia internet itu menguntungkan. Bayangkan, dimana lagi anda bisa mendapatkan *iPad* hanya dengan menembak bebek yang ada pada iklan-iklan di beberapa website? Dimana lagi anda mendapatkan *iPhone* karena dengan beruntungnya (atau lebih tepatnya seringkali) anda menjadi pengunjung ke 1000.000 di website tersebut? Semua hal tersebut gratis, dan yang anda perlukan adalah memberikan seluruh informasi personal anda. Selanjutnya, saya tidak tahu apa yang akan terjadi pada anda.

Wisudawan dan Google WPC/Lidya

Di sisi lain, dunia internet juga memiliki keunikan tersendiri. Saat saya sedang online *Facebook*, saya melihat *post* yang kurang lebih bertuliskan "Seorang anak kini sedang menderita penyakit Kanker dan harus mendapatkan perawatan intensif. Namun, karena keterbatasan biaya orang tua pasien, pihak Rumah Sakit hanya akan mengobati dan merawat pasien tersebut bila *post* ini mendapatkan 5000 like. Silahkan *re-post* dan sebarkan informasi ini demi kesembuhan anak tersebut". Bisa anda bayangkan bagaimana jumlah like dalam *post* tersebut dapat menjadi tolak ukur rasa kepedulian pada masyarakat? Bisa anda bayangkan bagaimana pihak Rumah Sakit harus menunggu post tersebut mendapatkan 5000 like untuk melakukan perawatan intensif pada pasien yang membutuhkan? Saya, tidak.

Yanuar Permadi

Data Kejahatan Tahun 2013

Lingkungan Univesitas Indonesia (UI) tidak pernah sepi dari pengunjung baik dari mahasiswa maupun warga sekitar yang hanya melintas. Karena ramainya masyarakat yang melintas maka kejahatan pun dapat terjadi.

Berdasarkan dari data yang didapat dari petugas keamanan kampus, dapat dilihat bahwa pada bulan November terdapat 10 kasus kejahatan. Pada bulan November kasus kejahatan yang terjadi meningkat dibandingkan bulan-bulan sebelumnya. Kejahatan yang terjadi diantaranya yaitu pencurian sepeda motor, pencongkelan kendaraan, pencurian lain-lain serta kasus kamtib lainnya. Yang paling banyak terjadi pada kasus pencurian tersebut yaitu terdapat pada kasus pencongkelan atau pencurian isi dalam kendaraan sebanyak 5 kasus. Selanjutnya pencurian kendaraan bermotor sebanyak 2 kasus, pencurian barang lainnya sebanyak 1 kasus. Lalu terdapat 2 kasus pada kegiatan kamtib lainnya.

Gusmara Agra, Yuriko Fitri

No.	Jenis Kasus	Bulan											JML
		JAN	FEB	MAR	APR	MEI	JUN	JUL	AGS	SEP	OKT	NOV	Total
1	Pemerasan	1	0	0	0	0	0	1	0	0	0	0	2
2	Pengeroyokan mengakibatkan luka	0	0	1	0	0	0	0	0	0	0	0	1
3	Penodongan	1	0	0	0	1	0	0	0	0	0	0	2
4	Penipuan/perbuatan curang	1	0	3	0	0	1	1	0	0	0	0	6
5	Pencurian sepeda motor	1	2	3	2	4	0	2	0	2	0	2	18
6	Pencurian dalam kendaraan/pencongkelan	0	0	1	0	3	0	0	0	2	0	5	11
7	Pencurian alat kantor	1	1	0	0	0	0	0	0	0	0	0	2
8	Pencurian sarana kampus	0	0	0	0	1	0	0	0	0	0	0	1
9	Pencurian di mesjid/mushola	1	0	3	0	0	0	0	0	0	0	0	4
10	Pencurian di dalam bus kampus	0	0	1	0	0	0	0	0	2	0	0	3
11	Pencurian lain-lain	0	0	1	1	1	0	1	0	0	1	1	6
12	Peursakan fasilitas kampus	0	0	1	0	0	0	0	0	0	0	0	1
13	pribadi	0	0	0	1	0	0	0	0	0	0	0	1
14	Penyalahgunaan Narkoba	0	0	1	0	1	0	0	0	0	0	0	2
15	Minum-minuan keras	0	0	0	1	0	0	0	0	0	0	0	1
16	Perbuatan asusila	1	0	0	2	1	0	2	2	1	0	0	9
17	Aksi kebut-kebutan	0	0	0	0	0	0	1	0	0	0	0	1
18	Kasus Kamtib lain-lain	0	0	2	2	0	0	0	0	0	0	2	6
Total		7	3	17	9	12	1	8	2	7	1	10	77


HIMPUNAN
Action, Through, Passion
HIMPUNAN MAHASISWA KRIMINOLOGI 2014

Utuh yang Setengah Part -3

Malam pun semakin mendekati pagi, aku bisa merasakan kantuk sudah menggelantungi mataku. Namun dalam hati ini ada bisikan yang menahan ku untuk tetap terjaga. Kedatangan dia malam tadi benar – benar janggal. Momen itu tak bias lepas dari rekam ingatanku. Setelah memantapkan hati, aku memutuskan untuk naik ke kamar tempat dia menginap untuk mengetahui keadaaan dan mengobati rasa khawatirku.

Ukiran besi berwarna emas bertuliskan "206" itu akhirnya ada di hadapanku. Meskipun samar – samar, dari celah pintu aku mengintip. Ternyata ruangan itu gelap gulita. Tak ada satupun lampu di dalam kamar yang menyala. Gemetar namun penuh keyakinan perlahan ku raih gagang pintu berusaha membukanya. Ternyata tidak terkunci. Begitu pintu itu terbuka, tercium bau amis darah yang sangat menyengat. Dengan susah payah, ku cari saklar lampu. Betapa terkejutnya aku, ketika kulihat dia tergeletak diatas kasur dengan bersimbah darah dan barang – barang berserakan. Meskipun hanya melihat di TV, aku langsung mengecek denyut nadinya. Lemah. Dia sekarat. Bergegas ku cari pesawat telp untuk memanggil staff yang lain.

"Tina! Ini Dani! Tolong dong kirim orang nih ke kamar 206... ada tamu yang sekarat nih."

"Ah yg bener, dan?! Jangan bercanda ah!" Tina tidak percaya.

"Iya! Buat apa sih gue bercanda jam segini. Ga ada untungnya tau! Tolong ya cepat! Oh ya! Hubungi ambulans juga ya." Aku mengakhiri pembicaraan.

Apa yang terjadi dengan dia? Mengapa sampai begini? Apakah pria tadi berniat membunuhnya? Ah! Benar – benar malam yang penuh pertanyaan. Tak lama kemudian Tina, Bapak Yoga, manager kami dan beberapa rekan Room Boy tiba. Kami memutuskan untuk membawa dia ke rumah sakit. Aku memutuskan untuk ikut menemani dia.

Perjalanan ke rumah sakit kami tempuh hanya dalam 10 menit karena kondisi jalan yang sangat sepi. Para petugas jaga IGD dan ambulans langsung membawa dia ke ruang IGD. Sedangkan aku menuju meja administrasi.

"Selamat malam mbak, saya mau daftarkan pasien"

"Oh! Yang barusan datang ya mas?"

"Iya mbak, tapi saya bukan keluarganya. Dia tamu hotel tempat saya bekerja." Tanyaku khawatir tentang administrasi dia.

"Gak apa – apa mas, yang penting ada data aja dulu." Jawab suster menenangkanku.

"Oh begitu ya mbak, oke deh. Nanti saya lengkapi datanya dari hotel ya mbak?" Tanyaku.

"Bisa, tapi sekarang boleh saya tau nama mas dan pasiennya?"

Pertanyaan suster barusan mengagetkanku. Berbulan – bulan aku tak pernah berani menanyakan nama dia. Dan sekarang aku tak bisa membantu dia hanya karena tidak tau nama dia.

"Saya Dani Darmawan, pasiennya....." Jawabku ragu.

"Siapa mas nama pasiennya?"

Tiba - tiba HP ku berdering. Kulihat nama TINA tertera di layar HP ku.

"Halo... Iya, Tin. Ada apa?" Aku bertanya heran.

"Gimana itu tamu yang tadi? Lo di RS kan sama dia?" Tanya Tina.

"Iya, ini gu di RS sama dia. Tapi gue belum tau keadaan dia. Dia masih di IGD. Eh, gue minta tolong dong?"

"Apa?" Sahut Tina.

"Lo masih di hotel kan? Coba deh cek data tamu kamar 206 itu. Siapa sih namanya?"

"AH! Jadi selama ini lo gak tau namanya siapa? Gue udah sampai rumah.. Sori gak bisa bantu sekarang, nanti siang deh ya. ok?" Jawab Tina.

"Oke deh!Sekarang NN aja dulu namanya deh. Makasih yaa....."

Tina menutup telepon. Perasaanku tak menentu, ku kembali menghampiri meja administrasi.

"Mbak, saya baru bisa kasih datanya nanti siang. Sekarang nama pasiennya NN aja bisa? Soal jaminan pakai nama saya aja ya? ini KTP saya." Sambil menyerahkan KTP ku.

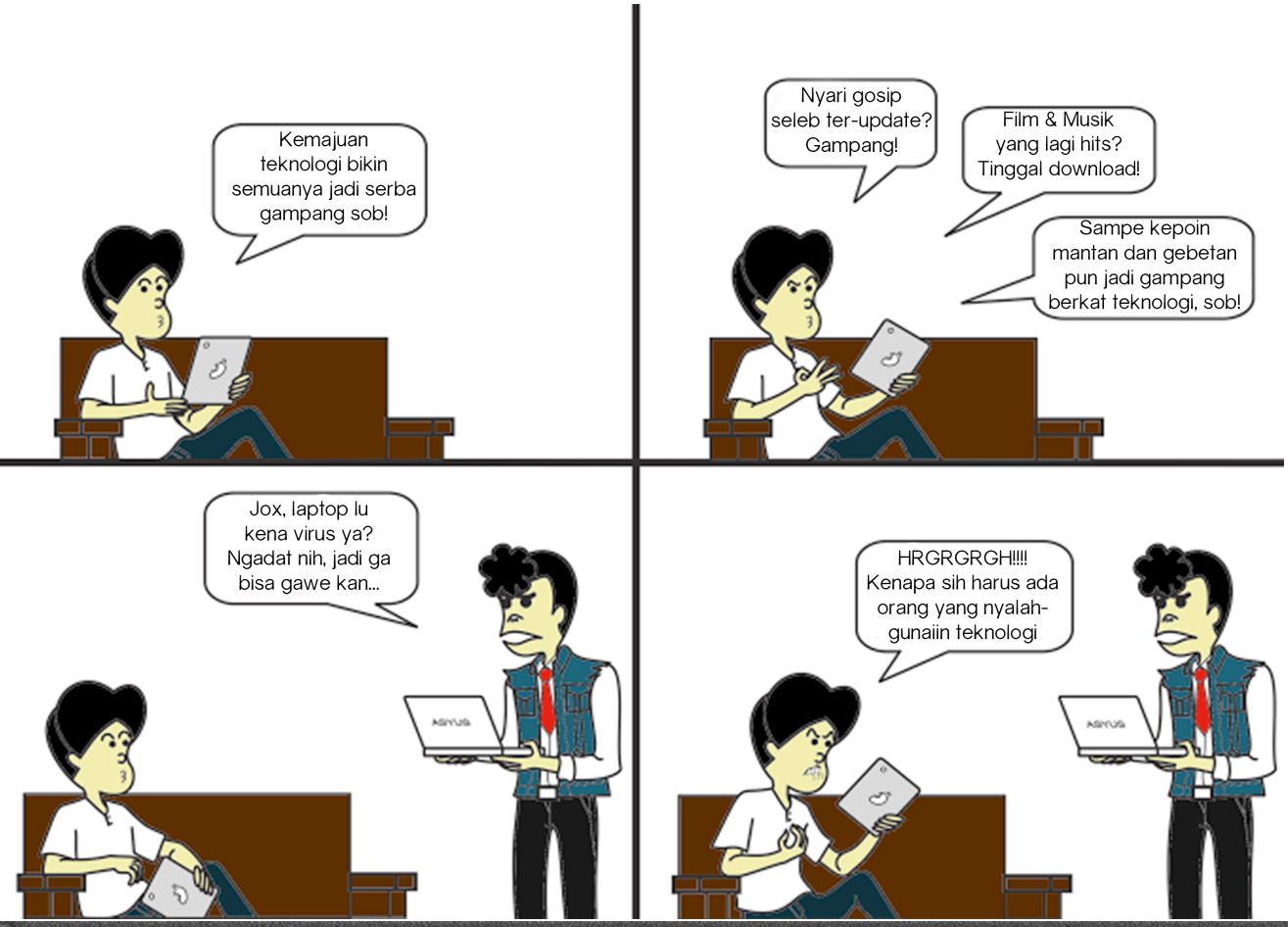
"Baik, silahkan ditunggu mas."

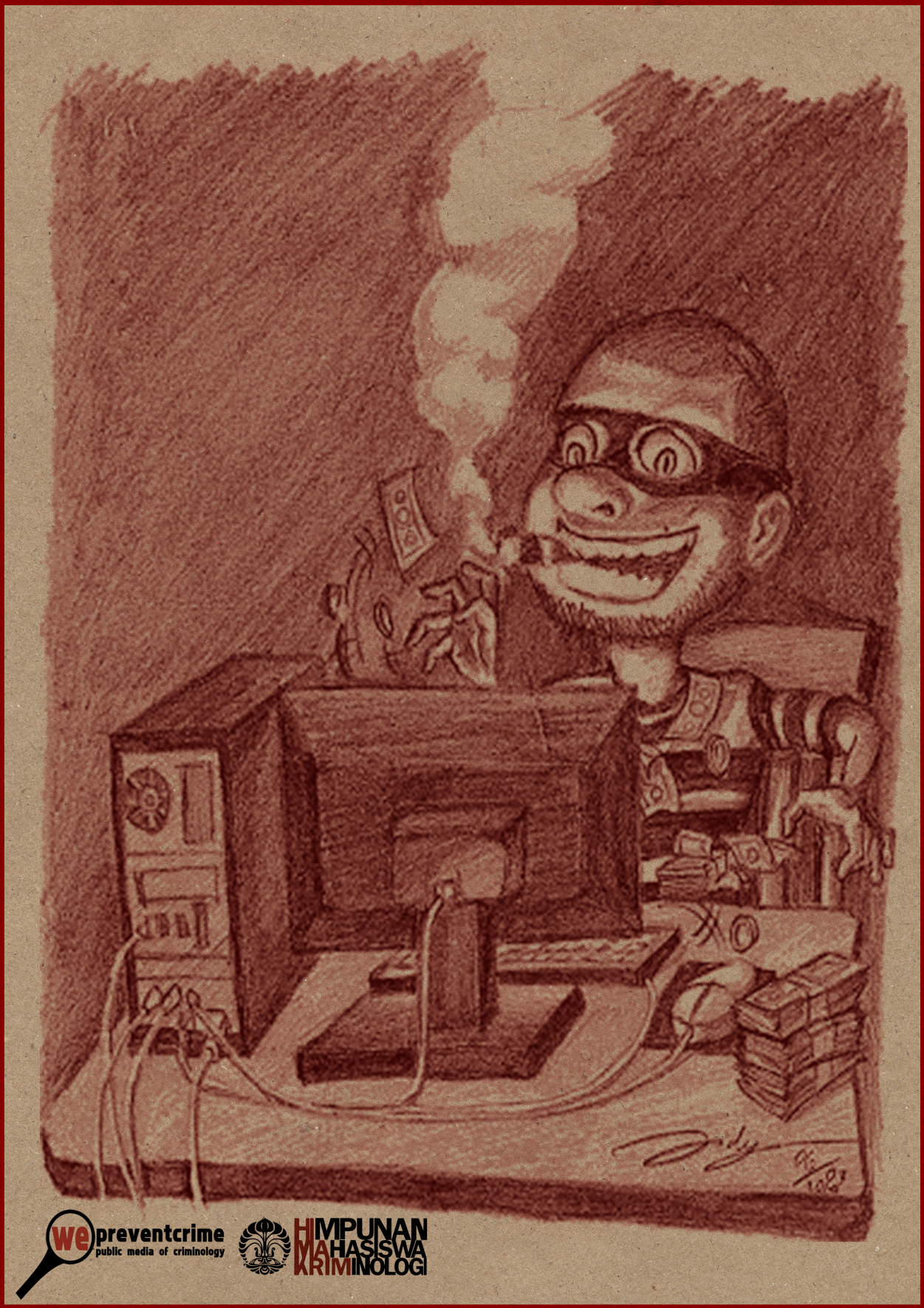
Di salah satu lorong sepi di rumah sakit itu, aku menunggu. Menunggu dokter menangani dia. Benar - benar hari yang melelahkan sekaligus tidak menyenangkan. Betapa tidak, kehadiran dia yang beberapa bulan kebelakang memberi warna baru dalam hidupku ternyata bisa berubah menjadi mimpi buruk yang menghantui ku hari ini, mungkin untuk seterusnya. Apakah dia akan baik - baik saja? Siapakah laki - laki yang tega melakukan ini padanya? Siapakah sebenarnya Dia? Semua pertanyaan itu lalu lalang di kepalaku. Namun, tersiarat setitik harapan bahwa dia akan baik - baik saja. Bahwa aku akan punya kesempatan untuk mengenalnya lebih jauh, merawatnya dan akhirnya punya kesempatan untuk menjawab semua pertanyaanku tadi. Di lorong sepi itu pun aku terlelap.

Bersambung...

Harris Kristanto

Salah Teknologi?





we preventcrime
public media of criminology

HIMPUNAN MAHASISWA KRIMINOLOGI