BAB III

DATA DAN KASUS MENGENAI TINDAK PIDANA *CYBER TERRORISM* DALAM TRANSAKSI ELEKTRONIK DI INDONESIA

A. Data *Cyber Terrorism* dalam Transaksi Elektronik di Indonesia

Ransomware WannaCry telah membuat heboh Indonesia karena sempat melumpuhkan sistem antrean rumah sakit. Meski keduanya telah kembali, Eko Widianto selaku Managing Director Bintang Anugrah Kencana yang merupakan distributor resmi F-Secure di Indonesia mengatakan kejadian ini adalah pembelajaran telat untuk meningkatkan kesadaran masyarakat akan bahaya *Ransomware*.

Menurut Eko, masuknya *ransomware* ke Indonesia karena kesadaran masyarakat yang masih rendah akan bahayanya. Selain itu, perilaku masyarakat yang suka membuka situs-situs dewasa juga menjadi penyebabnya," papar Eko saat ditemui CNNIndonesia.com di kawasan Senayan, Senin (15/5).[42]

Eko juga setuju dengan paparan Menkominfo Rudiantara beberapa waktu silam bahwa Indonesia merupakan sasaran terbesar dalam penyerangan siber. Menurut catatan Kominfo, ada 36,3 juta serangan dalam tiga tahun terakhir yang terjadi. Ini menurut Eko merupakan angka yang signifikan. Alasan Indonesia menjadi sasaran menurut Eko adalah masih karena rendahnya edukasi sehingga ada potensi besar korban tang terpancing *ransomware*. Seperti

[42] https://www.cnnindonesia.com/teknologi/20170515173827-185-214990/apa-penyebab-ransomware-masuk-indonesia di akses pada tanggal 7/22/2018 pukul 04:36

diketahui, modus kejahatan siber yang satu ini hanyalah mencuri data untuk mengancam korban agar memberikan sejumlah uang.

Di setiap kasus rata-rata kerugiannya 1,5-2 bitcoin yang kalau dikonversikan jadi sekira Rp23 juta per-bit coin. Itu baru dari segi material, kalau yang diserang rumah sakit bisa lebih bahaya. Misalnya rumah sakit kanker, mau operasi bagaimana kalau tidak ada datanya? Eko berkata. Sementara itu, pencipta *ransomware* sendiri sangat sulit ditemukan. Cara yang paling penting ditempuh adalah dengan melakukan tindakan pencegahan.

Kuncinya, pengguna internet harus menggunakan software yang update dan asli. karena yang diserang hanya mereka yang pakai *Windows XP*, padahal Microsoft sudah umumkan mereka tidak lagi dukung sistem operasi ini. Selain itu, kalau mau pilih antivirus, pilih yang ada teknologi *predict*, *prevent*, *detect* dan *respond*. Pelindung atau antivirus yang mampu memprediksi dan menganalisis serangan yang bakal dan sudah pernah dilancarkan peretas. Dengan kemampuan tersebut, sebuah antivirus akan mampu mencegah serangan yang akan datang dan mendeteksinya. Namun tak itu, antivirus yang patut Anda pilih harus mampu mengeksekusi atau merespon virus dengan baik sehingga dampak serangan pada sistem, data dan infrastruktur bisa diminimalisir atau dihilangkan sama sekali.

Hingga saat ini, belum ada satupun program yang mampu men-deskripsikan data yang telah dicuri *ransomware*. Oleh karena itu, Eko menyarankan pada pihak yang belum dan sudah terkena dampaknya untuk membiasakan diri mencadangkan data pada memori yang aman dari sentuhan koneksi internet.

Ancaman malware di Indonesia pada kuartal pertama 2018 diramaikan dengan ganasnya *Adware* 30,7 % dan *PUA Potentially Unwanted Application* 18,44 % yang menguasai hampir 50 % dari seluruh aktivitas *malware* di kuartal 1 tahun 2018. Disusul oleh gerombolan *Trojan* 11,68 %, *generic malware* 11,35 % dan *malware old* (lama) seperti *Sality*, *Ramnit* dan *Conficker* pada peringkat 5 sebanyak 10,42 %.[43]

Meskipun *Adware* dan *PUA* merajalela dan secara *de facto* menjadi raja *malware* karena paling banyak terdeteksi, namun *ransomware* seperti *Dharma* dan *Xorist* yang berdampak sangat menyusahkan korbannya karena mengenkripsi data penting komputer korbannya masih tetap ditemukan menjalankan aksinya dan memakan banyak korban di Indonesia dan berhasil menempati peringkat 9 *malware* yang paling banyak di Indonesia. Bagi anda yang mengaktifkan *Remote Desktop Protocol* untuk *server* anda, harap ekstra hati-hati menerapkan *TFA* dan membatasi *IP* yang bisa melakukan remote untuk mencegah pengambilalihan dan enkripsi oleh *ransomware*. Disiplinkan diri melakukan backup pada data penting anda secara teratur karena hanya backup teratur dan bukan program antivirus yang bisa menjamin keamanan data penting anda.

Selain itu, *malware miner* yang secara diam-diam melakukan penambangan Bitcoin / mata uang kripto menggunakan sumberdaya (listrik dan prosesor) komputer korbannya juga mengalami peningkatan seiring dengan tingginya popularitas Bitcoin dan mata uang kripto di tahun 2018 ini dan berada di peringkat 7 dengan total infeksi sebanyak 4,13 %.

Karena perkembangan teknologi *malware* yang sangat cepat, maka *malware* baru memiliki kemampuan yang sangat cepat dalam mengubah dirinya dan sangat sulit bagi anti-

[43] https://www.vaksin.com/statistik-malware-indonesia-q1-2018 di akses pada tanggal 7/22/2018 pukul 14:54

virus tradisional untuk mengikuti kemampuan *malware* yang sangat cepat merubah dirinya. Hal ini terlihat dari tingginya *generic malware* yang sebenarnya secara teknis masih belum pernah ditemui dan merupakan jenis *malware* baru, namun karena memiliki aktivitas yang mencurigakan, *malware* ini tetap berhasil dihentikan oleh *Webroot*.

Guna mengantisipasi *malware* yang tidak terdeteksi, ada baiknya para pengguna komputer mempertimbangkan menggunakan anti-virus yang memiliki kemampuan deteksi tinggi memanfaatkan teknologi real cloud sehingga dapat mendeteksi ancaman secara *realtime* tanpa tergantung pada update definisi antivirus lagi.

Tidak seperti jaman dulu dimana akan ada beberapa *malware* yang mampu menempati peringkat 10 besar *malware*, jenis *malware* yang beredar saat ini sangat banyak dan mencapai ratusan sehingga Vaksincom harus melakukan pemeringkatan berdasarkan kategori. Dan setiap kategori akan memiliki sub kategori ke setiap nama malware. Seperti diutarakan di atas, kategori malware yang paling banyak terdeteksi di Indonesia terlihat pada tabel di bawah ini:

NO	Malware	%
1	Adware	30.70%
2	PUA	18.44%
3	Trojan	11.68%
4	Generic	11.35%
5	Old	10.42%
6	Others	9.09%
7	Miner	4.13%

8	Hacktool	3.99%
9	Ransomware	0.20%
TOTAL		100%

B. Kronologi Kasus

Pada awalnya Kementrian Komunikasi dan Informatika Republik Indonesia (Kominfo) menyebut dua rumah sakit di Jakarta menjadi korban serangan siber *ransomware WannaCry*, yang juga melanda dunia. Dua rumah sakit yang dimaksud adalah Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais.

Ransomware yang menyerang kedua rumah sakit itu, berjenis *malicious software* atau *malware* yang menyerang komputer korban dengan cara mengunci komputer atau mengenkripsi semua data yang ada sehingga tidak bisa diakses kembali dan untuk guna membuka kembali data tersebut, korban harus membayar tebusan dalam bentuk Bitcoin.

Dia menyebut nyaris semua komputer di rumah sakit terpengaruh. *Ransonmware* itu mengunci semua data dan mengganggu sistem teknologi informasi yang menyimpan seluruh data kesehatan pasien juga catatan pembayaran rumah sakit. Saat ini, RS Dharmais tengah berupaya menginstal ulang sistem untuk membuat komputer dan server kembali beroperasi. Dia berharap proses tersebut cepat selesai karena kini rumah sakit beroperasi tanpa sistem teknologi informasi.

Bukan hanya rumah sakit di Indonesia saja yang menjadi korban, sistem jaminan kesehatan nasional Inggris (NHS) juga ikut terkena dampak *ransomware WannaCry* tersebut. Gambar yang beredar di media sosial menunjukkan layar komputer NHS dipenuhi tuntutan pembayaran tebusan dalam bentuk Bitcoin, senilai US$300. Mereka meminta pembayaran dilakukan dalam waktu tiga hari, atau harga tebusan akan berlipat ganda. Dan, bila tidak ada pembayaran dilakukan hingga tujuh hari, data akan dihapus. *Ransomware* berubah jadi mimpi buruk saat menyerang institusi seperti rumah sakit, yang bisa membahayakan nyawa orang," kata Kroustek, analis Avast.

Hal itu karena file yang terkunci membuat petugas kesehatan tidak bisa mengakses data pasien, sehingga prosedur operasi harus tertunda dan banyak pasien yang terjebak di rumah sakit. Selain rumah sakit, *ransomware* ini juga menyerang bank, perusahaan, layanan telekomikasi, serta layanan transportasi.

Ancaman teroris siber yang menyerang 99 negara dengan teknik ransomware ternyata ikut menimpa Indonesia. Bahkan, ada ribuan alamat internet protocol (IP) yang terinfeksi. Jumlah infeksi di Indonesia diperkirakan ribuan IP yang terdeteksi, dan Indonesia termasuk ke dalam salah satu negara yang terkena *Wannacry*.

Alasan rumah sakit tersebut terkena serangan *ransomware Wannacry* di karenakan sistem operasi *Windows* yang di pakai tidak melakukan menambal (*patch*) atau mempebaruhi (*update*) celah keamanan. Begitupun juga para masyarakat indonesia yang menjadi korban dari serangan *ransomware Wannacry* tersebut yang beberapa alat transaksi elektronik nya telah terkunci dan meminta tebusan dari serangan virus tersebut. Sebuah perusahaan keamanan *KnowBe4* melalui CEO-nya Stu Sjouwerman mengatakan bahwa rumah sakit

adalah target pemerasan yang sangat empuk oleh para peretas karena rumah sakit tidak fokus pada keamanan dunia maya. Sebaliknya, perhatian utama rumah sakit lebih menyentuh pada kepatuhan HIPAA (*Health Insurance Portability and Accountability Act*), sebuah hukum yang dibuat untuk menegakkan standar privasi data pasien terkait asuransi kesehatan, dalam konteks Amerika Serikat.

"Jika Anda mempunyai pasien, Anda pasti akan panik lebih cepat dibandingkan bila Anda menjual lembaran logam," kata Sjouwerman dikutip dari Wired.[44]

Saat *ransomware* menyerang sistem komputer di rumah sakit dan masyarakat indonesia, hal yang sebaiknya segera dilakukan adalah mematikan sebagian besar operasi jaringan, untuk mencegah tersebarnya kerusakan di *software-software* lain dan menyebar ke komputer lain.

C. Lembaga Pemberantasan *Cyber Terrorism*

1. Mabes Polri

Kepolisian Negara Republik Indonesia (Polri) adalah Kepolisian Nasional di Indonesia, yang bertanggung jawab langsung di bawah Presiden. Polri mempunya moto : Rastra Sewakotama, yang artinya Abdi Utama bagi Nusa Bangsa. Polri mengemban tugas-tugas kepolisian di seluruh wilayah Indonesia yaitu memelihara keamanan dan ketertiban masyarakat; menegakkan hukum; dan memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat. Polri dipimpin oleh seorang Kepala

[44] https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/ di akses pada tanggal 7/16/2018 pukul 12:54

Kepolisian Negara Republik Indonesia (Kapolri). Sejak 13 Juli 2016 jabatan Kapolri dipegang oleh Jenderal Polisi Tito Karnavian.

Organisasi Polri disusun secara berjenjang dari tingkat pusat sampai ke kewilayahan. Organisasi Polri tingkat pusat disebut Markas Besar Kepolisian Negara Republik Indonesia (Mabes Polri); sedang organisasi Polri tingkat kewilayahan disebut Kepolisian Negara Republik Indonesia Daerah (Polda) di tingkat provinsi, Kepolisian Negara Republik Indonesia Resort (Polres) di tingkat kabupaten/kota, dan Kepolisian Negara Republik Indonesia Sektor (Polsek) di wilayah kecamatan.

Dalam negeri, Kepolisian Republik Indonesia juga menghadapi banyak tantangan yang semakin kompleks seperti pemberantasan narkoba, korupsi dan pencucian uang, terorisme, *cyber crime*, perdagangan orang, kelompok-kelompok radikal dan intoleran. Kejahatan-kejahatan tersebut sudah bersifat transnasional dan memiliki jaringan global.

Dalam perkembangan paling akhir dalam kepolisian yang semakin modern dan global, Polri bukan hanya mengurusi keamanan dan ketertiban di dalam negeri, akan tetapi juga terlibat dalam masalah-masalah keamanan dan ketertiban regional maupun antarabangsa, sebagaimana yang ditempuh oleh kebijakan PBB yang telah meminta pasukan-pasukan polisi, termasuk Indonesia, untuk ikut aktif dalam berbagai operasi kepolisian, misalnya di Namibia (Afrika Selatan) dan di Kamboja (Asia).

2. Tugas dan Wewenang

Tugas pokok Kepolisian Negara Republik Indonesia adalah:

a. memelihara keamanan dan ketertiban masyarakat;

b. menegakkan hukum; dan

c. memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat.

Dalam melaksanakan tugas pokok sebagaimana dimaksud, Kepolisian Negara Republik Indonesia bertugas :

a. melaksanakan pengaturan, penjagaan, pengawalan, dan patroli terhadap kegiatan masyarakat dan pemerintah sesuai kebutuhan;

b. menyelenggarakan segala kegiatan dalam menjamin keamanan, ketertiban, dan kelancaran lalu lintas di jalan;

c. membina masyarakat untuk meningkatkan partisipasi masyarakat, kesadaran hukum masyarakat serta ketaatan warga masyarakat terhadap hukum dan peraturan perundang-undangan;

d. turut serta dalam pembinaan hukum nasional;

e. memelihara ketertiban dan menjamin keamanan umum;

f. melakukan koordinasi, pengawasan, dan pembinaan teknis terhadap kepolisian khusus, penyidik pegawai negeri sipil, dan bentuk-bentuk pengamanan swakarsa;

g. melakukan penyelidikan dan penyidikan terhadap semua tindak pidana sesuai dengan hukum acara pidana dan peraturan perundang-undangan lainnya;

h. menyelenggarakan identifikasi kepolisian, kedokteran kepolisian, laboratorium forensik dan psikologi kepolisian untuk kepentingan tugas kepolisian;

i. melindungi keselamatan jiwa raga, harta benda, masyarakat, dan lingkungan hidup dari gangguan ketertiban dan/atau bencana termasuk memberikan bantuan dan pertolongan dengan menjunjung tinggi hak asasi manusia;

j. melayani kepentingan warga masyarakat untuk sementara sebelum ditangani oleh instansi dan/atau pihak yang berwenang;

k. memberikan pelayanan kepada masyarakat sesuai dengan kepentingannya dalam lingkup tugas kepolisian; serta

l. melaksanakan tugas lain sesuai dengan peraturan perundang-undangan.

Dalam rangka menyelenggarakan tugas sebagaimana dimaksud Kepolisian Negara Republik Indonesia secara umum berwenang:

a. menerima laporan dan/atau pengaduan;

b. membantu menyelesaikan perselisihan warga masyarakat yang dapat mengganggu ketertiban umum;

c. mencegah dan menanggulangi tumbuhnya penyakit masyarakat;

d. mengawasi aliran yang dapat menimbulkan perpecahan atau mengancam persatuan dan kesatuan bangsa;

e. mengeluarkan peraturan kepolisian dalam lingkup kewenangan administratif kepolisian;

f. melaksanakan pemeriksaan khusus sebagai bagian dari tindakan kepolisian dalam rangka pencegahan;

g. melakukan tindakan pertama di tempat kejadian;

h. mengambil sidik jari dan identitas lainnya serta memotret seseorang;

i. mencari keterangan dan barang bukti;

j. menyelenggarakan Pusat Informasi Kriminal Nasional;

k. mengeluarkan surat izin dan/atau surat keterangan yang diperlukan dalam rangka pelayanan masyarakat;

l. memberikan bantuan pengamanan dalam sidang dan pelaksanaan putusan pengadilan, kegiatan instansi lain, serta kegiatan masyarakat;

m. menerima dan menyimpan barang temuan untuk sementara waktu.

Kepolisian Negara Republik Indonesia sesuai dengan peraturan perundang-undangan lainnya berwenang :

a. memberikan izin dan mengawasi kegiatan keramaian umum dan kegiatan masyarakat lainnya;

b. menyelenggarakan registrasi dan identifikasi kendaraan bermotor;

c. memberikan surat izin mengemudi kendaraan bermotor;

d. menerima pemberitahuan tentang kegiatan politik;

e. memberikan izin dan melakukan pengawasan senjata api, bahan peledak, dan senjata tajam;

f. memberikan izin operasional dan melakukan pengawasan terhadap badan usaha di bidang jasa pengamanan;

g. memberikan petunjuk, mendidik, dan melatih aparat kepolisian khusus dan petugas pengamanan swakarsa dalam bidang teknis kepolisian;

h. melakukan kerja sama dengan kepolisian negara lain dalam menyidik dan memberantas kejahatan internasional;

i. melakukan pengawasan fungsional kepolisian terhadap orang asing yang berada di wilayah Indonesia dengan koordinasi instansi terkait;

j. mewakili pemerintah Republik Indonesia dalam organisasi kepolisian internasional;

k. melaksanakan kewenangan lain yang termasuk dalam lingkup tugas kepolisian.

3. Unsur Pimpinan

Unsur pimpinan Mabes Polri adalah Kepala Kepolisian Negara Republik Indonesia (Kapolri). Kapolri adalah Pimpinan Polri yang berada di bawah dan bertanggung jawab kepada Presiden. Kapolri berpangkat Jenderal Polisi, Sejak 13 Juli 2016, Jenderal Badrodin Haiti diberhentikan dengan hormat dan digantikan oleh Jenderal Pol Tito Karnavian. Kapolri dibantu oleh seorang Wakil Kepala Polri berpangkat Komisaris Jenderal Polisi. Wakapolri saat ini dijabat oleh Komjen Pol Syafruddin

a. Unsur Pengawas dan Pembantu Pimpinan/Pelayanan

Unsur Unsur Pengawas dan Pembantu Pimpinan/Pelayanan terdiri dari:

1) Inspektorat Pengawasan Umum (Itwasum), bertugas membantu Kapolri dalam penyelenggaraan pengawasan dan pemeriksaan umum dan perbendaharaan dalam lingkungan Polri termasuk satuan-satuan organsiasi non struktural yang berada di bawah pengendalian Kapolri. Saat ini dipimpin oleh Komjen Pol Putut Eko Bayu Seno.

2) Asisten Kapolri Bidang Operasi (As Ops), bertugas membantu Kapolri dalam penyelenggaraan fungsi manajemen bidang operasional dalam lingkungan Polri termasuk koordinasi dan kerjasama eksternal serta pemberdayaan masyarakat dan unsur-unsur pembantu Polri lainnya. Asops saat ini dipegang oleh Irjen Pol Deden Juhara.

3) Asisten Kapolri Bidang Perencanaan Umum dan Anggaran (Asrena), bertugas membantu Kapolri dalam penyelenggaraan fungsi perencanaan umum dan pengembangan, termasuk pengembangan sistem organisasi dan manajemen serta penelitian dan pengembangan dalam lingkungan Polri. Saat ini dijabat oleh Irjen Pol Bambang Sunarwibowo

4) Asisten Kapolri Bidang Sumber Daya Manusia (AS SDM), bertugas membantu Kapolri dalam penyelenggaraan fungsi manajemen bidang sumber daya manusia termasuk upaya perawatan dan peningkatan kesejahteraan personel dalam lingkungan Polri. Saat ini dijabat oleh Irjen Pol Arief Sulistyanto.

5) Asisten Kapolri Sarana dan Prasarana (Assarpras), bertugas membantu Kapolri dalam penyelenggaraan fungsi sarana dan prasarana dalam lingkungan Polri. Assarpras dijabat oleh Irjen Pol Asep Suhendar.

6) Divisi Pertanggungjawaban Profesi dan Pengamanan Internal (Div Propam), adalah unsur pelaksana staf khusus bidang pertanggungjawaban profesi dan pengamanan internal. Kadiv Propam saat ini ialah Irjen Pol Martuani Sormin.

7) Divisi Hukum (Div Kum), dengan pimpinan Irjen Pol Raja Erizman.

8) Divisi Hubungan Masyarakat (Div Humas), dengan pimpinan Irjen Pol Setyo Wasisto.

9) Divisi Hubungan Internasional (Div Hubinter), adalah unsur pembantu pimpinan bidang hubungan internasional yang ada di bawah Kapolri. Bagian ini membawahi National Crime Bureau Interpol (NCB Interpol), untuk menangani kejahatan internasional. Dengan pimpinan Irjen Pol Saiful Maltha.

10) Divisi Teknologi Informasi dan Komunikasi Kepolisian (Div TIK Pol), adalah unsur pembantu pimpinan di bidang informatika yang meliputi teknologi informasi dan komunikasi elektronika. Dipimpin oleh Irjen Pol Prasta Wahyu Hidayat.

11) Staf Pribadi Pimpinan (Spripim)

12) Sekretariat Umum (Kasetum). Dipimpin oleh Kombes Pol Ratnawati Hadiwidjaja.

13) Pelayanan Markas (Kayanma). Dipimpin oleh Kombes Pol Budi Widjanarko.

14) Staf Ahli Kapolri, bertugas memberikan telaahan mengenai masalah tertentu sesuai bidang keahliannya

4. Hasil Wawancara

Untuk melengkapi hasil dari penelitian tersebut penulis melakukan wawancara dengan suatu divisi di Mabes Polri yang dilakukan oleh seorang anggota kepolisian. Bahwa menurut anggota kepolisian tersebut untuk kasus yang telah terjadi di rumah sakit di jakarta yang telah menjadi korban serangan virus *ransomware Wannacry* tersebut merupakan tindakan *cyber terrorism*. Berikut adalah pertanyaan – pertanyaan yang penulis ajukan kepada anggota kepolisian yang bergerak pada divisi tersebut.[45]

1. Bagaimana serangan *virus ransomware Wannacry* yang telah terjadi di rumah sakit di jakarta dapat di katakan sebagai tindakan *cyber terrorism*?

   Jawaban: Serangan yang telah terjadi di rumah sakit tersebut dapat di katakan sebagai tindakan *cyber terrorism* di karenakan serangan tersebut bersifat ancaman atau teror yang dimana ancaman tersebut telah meresahkan masyarakat luas atau fasilitas tersebut serta mengakibatkan kerusakan atau kehancuran terhadap objek-objek di rumah sakit tersebut seperti dalam contoh komputer – komputer yang ada di rumah sakit tersebut menjadi tidak berfungsi akibat serangan virus *ransomware Wannacry* tersebut.

2. Bagaimana cara mengidentifikasi bahwa pelaku yang menyerang rumah sakit di jakarta telah melakukan tindakan *cyber terrorism*?

   Jawaban: Pelaku dapat di identifikasi kan telah melakukan tindakan *cyber terrorism* pada serangan rumah sakit tersebut, dan dapat di lihat dari aksinya yang melakukan penyadapan kepada komputer – komputer di rumah sakit tersebut yang dimana penyadapan tersebut bersifat pelaku meminta tebusan bitcoin dan pelaku telah melakukan

[45] Wawancara dengan anggota mabes polri, 5 Juli 2018 di Mabes Polri, Jakarta Selatan

ancaman atau teror untuk menghilangkan seluruh data di rumah sakit tersebut jika keinginan nya tidak terpenuhi.

3. Bagaimana pelaku dapat melakukan aksinya berupa serangan di rumah sakit tersebut?

Jawaban:

a. Komputer sebagai alat yang digunakan lalu dengan teknik memberi virus bersifat *malware* dimana virus ini dapat menyebar dengan cepat sehingga telah menginfeksi sesuai target yang di inginkan.

b. Sistem keamanan komputer pihak rumah sakit yang tidak di perbaharui (update) sehingga pelaku dapat dengan mudah memasuki atau menyadap keamanan tersebut.

c. Target, dalam hal ini pelaku kejahatan mengadakan konsolidasi dan koordinasi dalam melakukanan sasaran aksi terornya, misalnya pada kasus laptop milik pelaku kejahatan bom bali setelah dilakukan *decrypt* terbukti internet dipakai untuk mengadakan koordinasi pada aksi teror dan targetnya.

4. Bagaimana penanganan penyidik dalam menangani kasus *cyber terorrism* di indonesia?

Jawaban: Narasumber mengatakan bahwa dalam menangani kasus tersebut di gunakan nya pendekatan *cyber*, yang artinya bahwa melakukan *counter cyber terrorism*, yang terdiri dari *cyber patrol* (patroli dunia maya) , *cyber attack* (serangan siber), dan *cyber surveillance* (pengawasan siber). Patroli siber tersebut dilakukan oleh tim pasukan siber yaitu dengan memantau aktivitas atau pergerakan jaringan terorisme lewat dunia maya. Lalu adanya tim *cyber army/cyber troops* (pasukan siber), mereka tiap hari kerjanya

hanya membaca website. Dalam memantau laman website, tim tersebut melakukan pelacakan terhadap situs yang menjadi komunikasi para teroris di dunia maya.

Kemudian ketangkap suatu nanti ada *chatting room* nya, mereka kemudian *chatting room* nya diikuti masuk lalu gabung dengan mereka itu di antaranya. Pelacakan itu tersebut juga dapat dilakukan terhadap alat pengiriman pesan seperti whatsapp dan telegram. Teknik-teknik *cyber patrol* ini juga sama sebenarnya dengan teknik-teknik dalam dunia nyata ada yang menggunakan *surveillance* (pengawasan) nyata.

Setelah masuk dalam obrolan komunikasi jaringan teroris itu, pihak kepolisian melakukan penyamaran untuk masuk seolah-seolah menjadi bagian kelompok-kelompok teroris dengan menggunakan berbagai akun termasuk ikut *chatting* dalam komunitas mereka. Sebagian besar terdeteksi tapi mereka juga sebagian besar berusaha menghindari deteksi intelijen dengan menggunakan metode-metode termasuk sistem komunikasi mereka.

5. Upaya apakah yang dilakukan untuk melindungi atau menanggulangi dari tindakan *cyber terrorism*?

Jawaban: Narasumber mengatakan untuk saat ini mereka mempunyai tim khusus yang dimana tim khusus ini telah melakukan *undercover*, lalu jika masyarakat telah melihat atau merasakan ancaman atau teror melalui dunia maya segera lah untuk melaporkan kejadian tersebut ke pihak kepolisian. Serta jika melihat kasus yang telah terjadi di rumah sakit di jakarta untuk mencegah terinfeksi virus *ransomware Wannacry*, di haruskan perbaharui sistem keamanan dalam komputer atau transaksi elektronik lain nya begitu pun juga perbaharui anti-virus ataupun dengan cara membeli produk original. Untuk

langkah lebih aman nya di sarankan untuk melakukan back up data-data yang penting sehingga jika data tersebut telah hilang terkena serangan virus tersebut dapat di kembalikan dengan mudah.