Digital Investigations. Dutch Perspective

RICHARD VRIESDE

Jefe ITCU. Policía Nacional de Holanda

1. Introduction

Internet is gaining ground in the Netherlands too. The number of Internet connections is on the increase and a growing number of companies are making use of Internet. In about two years' time, Internet will be available through the television cable, which will make it possible for every TV owner to access the Web, whose coverage will be extended enormously by then.

Internet's role in the functioning of the police and judiciary in the Netherlands will be ever greater.

1.2 Internet and the Dutch police

Using the Web as an investigation tool is a relatively new facility for the Dutch police.

The speed with which the technological developments take place these days requires continuous attention for adjustments in the practice of investigation.

Case law, too, plays sometimes an important part in determining what the Dutch police may and may not do under certain circumstances in the practice of digital investigations.

Due to the non-physical character of the digital environment, where atoms have been replaced by bits and bytes, it is sometimes hard to interpret the present legal frameworks. The changes that take place make it necessary for the police and justice authorities to ask themselves what these changes mean for investigation and prosecution.

I should like to stress that the contents of this presentation refer to a developing situation. The Dutch police's use of Internet as an investigation tool must still be developed in many respects.

On the other hand, I expect that the current and future Dutch legislation, offers some legal security for the longer term.

2. Co-operation between the police and the judiciary

2.1 Organisational structure of law enforcement agencies

Even before the introduction of the Computer Crime Act (1993), the Dutch police had started specialist teams for the fight against computer crime. In 1992, after successful pilot projects in The Hague, Amsterdam, and Nijmegen, the minister of Justice and the minister of the Interior decided to install a national network of interregional computer crime teams. All five districts now have their own team.

The computer crime teams closely co-operate with the forensic computer research unit of the Forensic Laboratory and the Information Technology and Crime Unit of the CRI.

2.2 Computer Crime Policy Advisory Group

In 1994 the Computer Crime Policy Advisory Group was set up in the Netherlands. Its task is to identify the consequences of the rapid developments in the information technology on the functioning of the police and the judiciary. The policy advisory group directs the activities in the field of technology, the

development of methods and procedures, innovation, education, police and legal matters.

The policy advisory group is composed of the team-leaders of the five interregional computer crime teams, representatives of the Ministry of Justice, representatives of the Dutch National Criminal Intelligence Division (CRI), of the Forensic Laboratory and the Crime Investigation Training School. Recently, they were joined by the Technical Support Division of the National Police Agency.

This was the start for a network covering Dutch territory for the suppression of computer crime at national level.

2.3 1996 Report

In 1996 the police advisory group presented the Council of Chiefs of Police with the report 'Towards .... digital crime investigations'.

The report states that the developments in the information technology take place in rapid succession and have direct impact on society. The individual citizen can use the electronic payment and banking system. Companies can benefit from the quick means of communication and from working at distance. In general, the conclusion is that, owing to the information technology, traditional forms undergo changes and entirely new types of crime emerge.

2.4 Open sources

Another development in which the Dutch police is making large investments is the use of (digital) open sources. Using information sources is nothing new in the suppression of crime. For years now, the police have used books, magazines and papers. These days, other sources (as you can see on this slide) are available as well, often electronic ones. Therefore, ABRIO - a programme developed by the Dutch police - pays much attention to consulting open sources via Internet.

3. The Police, E-highway and law enforcement

The current coalition Government in the Netherlands has decided to take the electronic highway seriously. In December 1994, the national plan of action on electronic highways 'From metaphor to action' was introduced. Several ministries started out from the plan, among them the Ministry of Justice with the project 'Principles for legislation along the electronic highway'.

Several aspects are of importance to the Police.

The Computer Crime Act of 1993 was the legislators' answer to the new developments in information technology. This act is still a good tool, but now, in 1997/98, it can well be argued that the legislators, as well as the majority of hardware and software industries, could not foresee the explosive growth of computer networks and functional integration of telecommunication systems. This is why in the near future the possibilities and limitations of investigations pertaining to computer networks (such as the Internet) must be carefully examined, and, if necessary, adapted.

As you can see we don't have problems, only challenges!

Here are a number of interesting challenges for legislators and judicial authorities.

3.1 The first challenge: judicial competence

The first challenge is that of judicial competence. On the one hand, the acts punishable under the Criminal Code are based on locality (scene of the crime, location of offender and victim), on the other hand, the locality of the Internet is the world, so, any place on earth. Currently, 168 countries are connected to the Internet and transmission through anonymous FTP and remailers make it very difficult for the police to trace computer crimes.

The afore-mentioned problems are not limited to hackers on the Internet. As more and more information is stored in computers, criminal investigators will have a growing need of accessibility of computerised evidence, in hacking cases, in cases against drugs dealers who keep information on their transactions in the computer, and so on. Often, however, it will be difficult to gain access, because when investigators apply for a search warrant, they are obliged to specify the

location of the evidence (search warrants must be applied for in the same area of judicial competence as where the evidence is kept).

International fraud on the Internet will force countries to pay attention to subjects such as: where will the criminal appear before a court, who has judicial competence, and can we acknowledge the damage caused in other countries?

3.2 The second challenge: identity

Another issue in the fight against cyber crime is identification. Who is who? The commercial world is very much in favour of digital authographs, a password used in combination with a mathematical formula, an encryption algorithm. This is excellent for commercial purposes, but not for criminal investigators, because a user's digital autograph can easily be discovered by other users of the same computer, be they relatives, friends, or colleagues.

The Internet carries no biometric evidence; there are no unique characteristics such as handwriting or voice that may lead to a successful prosecution. Users are virtually anonymous.

The electronic signature will certainly play an important role in the future. And I fully agree on that with the presentation of mr. Richard Giles last Thursday. It is important for the authorities and society as a whole that this will be correct and fraud-resistant.

3.3 The third challenge: technological developments

The third challenge is posed by technological developments. One characteristic of authorities and police services is that they are very slow to adapt to new developments. Internet, however, makes it ridiculous to go on as they have always done. Encryption, for example, protects privacy and helps commerce; in this way, information can be protected against hackers, but criminals also make use of encryption, in terrorist activities, in child pornography, by hackers themselves. This means that ways of encryption must be developed which can be broken, if necessary by law enforcement.

4. Internet related crime (traditional)

Many data-related offences on Internet come down to undesirable publication (or copying). Data-related crimes such as child porn, racism and copyright infringements have that aspect in common.

4.1 Hotline against child pornography

The NLIP, the association to which most Internet providers in the Netherlands belong, created the Internet hotline against child pornography in the middle of 1996. The police was involved in the creation of this centre from an early stage and CRI's Information Technology and Crime Department actively participated. For a long time, contacts have existed with the XS4ALL, an Amsterdam based Internet provider, which actively supports the hotline.

Although the hotline is meant to lead to more effective and efficient suppression of child porn on Internet, a first evaluation by the CRI showed that there are reasons to doubt its effectiveness.

The creation of the hotline has only had limited effect on the flow of child porn that is available on Internet in the Netherlands. The reason is that the hotline can only act if the source is known and if the source is from the Netherlands itself.

On this slide you can see some statistics from this year published by the hotline. (reports on e-mail 82: of which 75 refer to 2 mass-e-mailings)

Though the Internet Hotline against Child pornography aims do not include taking action against childpornography originating in other countries, the hotline passed 7 reports to the police. The seriousness of the reports was regarded as sufficient grounds to pass them on. In the near future, the procedure regarding foreign reports will be changed.

In a number of cases in other countries, particularly Japan, child pornography was distributed on the Internet and the author claimed that this was permissible according to local norms.

Moreover, self regulation in case of non-compliance is limited. A mechanism is required to enable action from the authorities, with criminal action as the concluding factor in a series of measures taken to suppress the distribution of child porn on Internet.

Also, in the Netherlands, the developments in the business sector in Britain, in consultation with DTI and the police in the R3 Safetynet and other international developments (e.g. PICS - Platform for Internet Content Selection) are followed closely.

4.2 Internet hotline against racism

Next to the hotline against child pornography, a hotline against racist publications on the Internet was established in February 1997 by national anti-racism organisations.

4.3 New types of Internet-related crime

The following are some recent examples of new types of on-line crime in the Netherlands.

Criminals massively on-line - In April this year, hooligans of football club PSV made an invitation via Internet to Ajax supporters to a fight. The invitation was relayed through two Dutch Internet providers. The justice authorities have demanded that the providers disclose the identity of the authors, but it is by no means certain that they will succeed. Someone may pass himself off as someone else and still be able to distribute messages inciting to violence. There are numerous ways to remain anonymous on Internet, also at the expense of someone else.

But also, shrewder individuals wishing to distribute controversial messages (calling for violence, publishing child porn, or racist texts) and exploiters of illegal casinos rather use computers abroad, which do not come under Dutch legislation.

Snuff pictures on Internet - Internet is also used to distribute very gruesome and morbid pictures in digital form of people being killed. These images are not punishable in the Netherlands, unless the court decide otherwise when it is distributed to children under the age of 16.

In brief, with the advance of technology, there are growing numbers of possibilities for the individual to compose images with contents that cannot be distinguished from 'real'.

Also, new payment facilities through Internet may lead to use for criminal purposes, including money laundering.

Other Internet crimes that are likely to emerge are:

- gambling via Internet, often by using encryption

- terrorist use of Internet.

Apart from the physical threat, there is the virtual threat.

4.4 Illegal use of new technology in the Netherlands

The following illegal use of new technology has already been seen in the Netherlands:

- the use of techniques aimed at counter-observation (sounding out)
- the interception of e-mail messages
- the hacking of computers with Internet connection
- the interception and tapping of semaphones
- the tapping of mailboxes connected to ATF and GSM networks
- the abuse of packet radio (from prison)
- the abuse of *21
- the tapping of scope card numbers given to call centres through phone boxes
- the tracing of PIN codes through the H (repeat) key; in hotels pincodes given over the phone are often stored centrally

4.5 Remarking Intel SYMBOL 210 \f "Symbol" \s 12 Pentium Processors

Another problem is the remarking of Intel Pentium processors. (As you might know, remarking is the unauthorized removal of e.g. Intel Trademarks and chip identification from the surface of the processor package and remarking with incorrect identifiers.) In the most recent case Pentium Processors tested to 100Mhz, where remarked as 166 Mhz parts. Very special and expensive equipment was used by the processing.

4.6 Illegal trade of SIM cards

The illegal trade of SIM cards is one of the excrescences of the booming market of mobile phones. In the fierce competition to obtain a large market share (in the Netherlands, a portable phone is often cheaper than a loaf of bread), companies frequently fail to introduce proper security measures. A criminal will not have to exert himself to circumvent the superficial check of biographical data: many phone shops accept a photocopy of a passport or driving licence which the future customer has brought himself.

Pocket phones provide criminals with an opportunity to do lucrative business. Obviously, when a complaint has been made to the police, the numbers in question are blocked, but the phones themselves can still be sold in other European countries, even without a SIM card. In these countries, customers are not lured with (almost) free pocket phones, but they are sold for hundreds of guilders. Here, subscriptions are taken without a phone; later such an phone will be bought on the black market.

4.7 Pre-paid phone cards

Another development which causes worry to the authorities, is the increasing use of (pre-paid) phonecards, which makes making a call even more anonymous than it used to be. In most European countries, in line with privacy regulations, the cards and their users are not registered.

5. International (police) cooperation

As we have heard many times this conference, Internet-related crime is cross border crime, which makes international co-operation a necessity. The approach to computer crime is different for each country, the investigation and prosecution methods that are used may be similar.

Global co-operation is needed to successfully fight against cyber crime. It should be possible to ask a country's assistance even if crime has not taken place there, the perpetrator is not staying there, and there are no victims in that country, simply because relevant data can only be found there. An effective fight against computer crime depends on two conditions: co-operation among countries and a

preparedness to gear national legislation and adapt it to the new digital possibilities.

5.1 Interpol Working Group on Information Technology and Crime

At international level, the Interpol Working Group on Information Technology and Crime attempts to promote international standardisation of methods, procedures and harmonisation of legislation. As we've heard from Phil Swinburne yet.

Another important organisation at international level in the combat of computer crime is the international organisation of Computer Evidence (IOCE).

5.2 Dutch presidency of the European Union

The Dutch presidency has set out to make an inventory of the activities undertaken with respect to Internet. To that end, the Working Party on Illegal and Harmful Content on the Internet has been set up under the chairmanship of the European Committee, as said yesterday by mr. Berend Jan Drijber.

Moreover, on 29 November 1996 the Stop programme was adopted, which provides for suppressive action against the use of Internet for illegal activities, such as child porn and inciting to racial hatred.

Conclusion

My conlusion is very short.

In my opinion: Any law will be without practical effect if an offender cannot be held responsible.

Thank You

Investigaciones Digitales. La Perspectiva Holandesa*

RICHARD VRIESDE

Jefe ITCU. Policía Nacional de Holanda

1. Introducción

Internet está ganando terreno en los Países Bajos. El número de conexiones a Internet está en aumento y un número creciente de compañías hacen también gran uso de Internet. Dentro de dos años aproximadamente, Internet estará disponible mediante el cable televisivo, que hará lo posible para que cada propietario de TV pueda acceder al WEB, y cuya cobertura se extenderá enormemente.

El papel de Internet y el funcionamiento de los policías y el juzgado en los Países Bajos, aumentará considerablemente.

* Traducción del artículo anterior, realizado mediante el programa Power Translator Profesional.

1.2 Internet y los policías Holandeses

Usar la WEB como una herramienta de investigación es relativamente una nueva facilidad para los policías Holandeses.

La velocidad con que los desarrollos tecnológicos tienen lugar estos días requiere atención continua para ajustes en la práctica de investigación.

El derecho común, demasiado a veces juega una parte importante en determinar qué los policías Holandeses pueden y no pueden hacer bajo circunstancias seguras en la práctica de investigaciones digitales.

Debido al no-físico carácter de ambiente digital, donde átomos han sido reemplazados por octetos, a veces es duro interpretar las estructuras legales actuales. Los cambios que tienen lugar son necesarios para que las autoridades de justicia y policías puedan aumentar la investigación y enjuiciamiento.

Quisiera acentuar que el contenido de esta presentación se refiere a una situación creciente. El uso de policías Holandeses en Internet como una herramienta de investigación debe todavía desarrollarse en muchos aspectos.

Por otra parte, espero que la actual y la futura legislación Holandesa, ofrezca alguna seguridad legal a largo plazo.

2. Co-operación entre los policías y el juzgado

2.1 Organización de la estructura de agencias de ejecución de la ley

Antes de la introducción en el Crimen de Computadora (1993), los policías Holandeses habían comenzado a especializarse y unirse para la lucha contra el crimen de computadora. En 1992, después del proyecto piloto exitoso en El Hague, Amsterdam, y Nijmegen, el Ministro de Justicia y el Ministro del Interior decidierón instalar una red nacional interregional y equipos de crimen de computadora. Estos cinco distritos ahora tienen sus propios equipos.

Los equipos de crimen de computadora cooperan estrechamente con las unidades forenses de investigación de computadora del laboratorio forense y el Crimen y Tecnología de Información Unidad del CRI.

2.2 Crimen de Computadora Grupo Político Consultivo

En 1994 el Grupo Político Consultivo sobre el Crimen de Computadora se estableció en los Países Bajos. Su tarea era identificar las consecuencias de los desarrollos rápidos en la tecnología de la información sobre el funcionamiento de los policías y el juzgado. El grupo político consultivo administra las actividades en el campo de la tecnología, el desarrollo de métodos y procedimientos, innovación, educación, policías y materias legales.

El grupo político consultivo se compone del equipo - los líderes de los cinco grupos, representantes del Ministerio de Justicia, representantes de la División de Inteligencia Criminal Holandesa Nacional (CRI), del laboratorio forense y la Escuela de Capacitación de Investigación de Crimen. Recientemente, ellos eran reunidos por la División de soporte técnico de la Agencia Nacional de Policías.

Este era el comienzo para una red que cubre el territorio Holandés para la supresión de crimen de computadora a nivel nacional.

2.3 Informe 1996

En 1996 los policías del grupo consultivo presentaron el Consejo de jefes de policía con el informe 'Towards .... investigaciones sobre el crimen digital.

El informe declara que los desarrollos en la tecnología de la información tienen lugar en la sucesión rápida y tienen impacto directo sobre la sociedad. El ciudadano individual puede usar el sistema bancario y pago electrónico. Las compañías pueden beneficiarse de los medios rápidos de comunicación y de trabajar a distancia. En general, la conclusión es que, debido a la tecnología de la información, las formas tradicionales experimentan cambios y surgen nuevos tipos de crimen.

2.4 Fuentes abiertas

Otro aspecto en el que los policías Holandeses realizan actuaciones es el uso de (digital) fuentes abiertas. Usar las fuentes de informe no es algo nuevo en la supresión de crimen. Desde hace años, los policías han usado libros, revistas y papeles. Hoy día, las otras fuentes (como se puede ver sobre esta diapositiva) están disponibles también, frecuentemente en soporte electrónico. Por lo tanto, ABRIO - un programa desarrollado por los policías Holandeses - suscita mucha atención para consulta de fuentes abiertas por medio de Internet.

3. Los Policías, E-highway y ejecución de la ley

El Gobierno actual de coalición en Países Bajos ha decidido seguir el camino de las autopistas electrónicas seriamente. En Diciembre 1994, se puso en marcha el plan nacional de acción sobre autopistas electrónicas "From metaphor to action". Los distintos ministerios comenzaron en este aspecto, entre ellos el Ministerio de Justicia con el proyecto "Principles for legislation along the electronic highway".

Los distintos aspectos son de gran importancia para los Policías.

El Acta de Crimen de Computadora de 1993 fue la contestación de los legisladores a los nuevos desarrollos en la tecnologías de la información. Este acta es todavía una buena herramienta, pero ahora, en 1997/98, puede que los legisladores, así como también la mayoría de las industrias de software, no han podido prever el crecimiento explosivo de redes de computadora e integración funcional de sistemas de telecomunicación. Esto es por qué en el futuro próximo las posibilidades y las limitaciones de investigaciones en las redes de computadora (tal como Internet) deben cuidadosamente reconocerse, y, si es necesario, adaptadarse.

3.1 Recusación primera: la capacidad judicial

La recusación primera es la de capacidad judicial. Por un lado, los actas punibles en el código criminal son base en la localidad (escena, localización de injuriador y víctima), por otra parte, la localidad de Internet es el mundo, cualquier lugar sobre la tierra. Actualmente, 168 países se conectan al Internet y la transmisión mediante FTP anónimo y emailers lo hace muy difícil para que los policías investigen crímenes de computadora.

Los mencionados problemas no están limitados a los hackers sobre Internet. A más información almacenada en las computadoras, los investigadores criminales tendrán una necesidad creciente de acceso automatizado, en causas contra negociantes de drogas que informe de la manutención sobre sus negocios en la computadora. Frecuentemente, sin embargo, será difícil ganar acceso, porque cuando los investigadores aplican un mandamiento de registro, ellos se obligan a especificar la localización de la evidencia (los mandamientos de registro deben aplicarse para la misma área de capacidad judicial hacia donde la evidencia se guarda).

El fraude Internacional sobre el Internet forzará a los países a prestar atención a cuestiones tales como: ¿dónde comparecerá el criminal, quién tiene capacidad judicial, y podemos nosotros admitir que daño causó en otros países?

3.2 La segunda recusación: la identidad

Otra emisión en la lucha contra el cybercrimen es la identificación. ¿Quién es quién?. El mundo comercial está mucho a favor del autógrafo digital, una contraseña basada en la combinación con una fórmula matemática, un algoritmo de encriptación. Estos es óptimo para propósitos comerciales, pero no para investigadores criminales, porque un autógrafo digital de usuario puede fácilmente ser descubierto por otros usuarios de la misma computadora, ser ellos parientes, amigos, o colegas.

Internet no conlleva evidencia biométrica; no hay características únicas tal como escritura o voz que puede conducir a un enjuiciamiento exitoso. Los usuarios son virtualmente anónimos.

La firma electrónica jugará seguramente un papel importante en el futuro. Y estoy totalmente de acuerdo con la presentación de Mr. Richard Giles el pasado Jueves. Es importante para las autoridades y la sociedad mientras exista un fraude resistente.

3.3 La tercera recusación: los desarrollos tecnológicos

La tercera recusación está basada en los desarrollos tecnológicos. Una de las características de los servicios policiales y autoridades es que ellos se demoran mucho para adaptarse a los nuevos desarrollos. La encriptación, por ejemplo, protege la intimidad y ayuda al comercio; de esta manera, el informe puede protegerse contra hackers, pero hay criminales que también hacen uso de modelos de encriptación, en actividades terroristas, en la pornografía infantil, como hackers en sí mismos. Esto significa que las maneras de encriptación deben desarrollarse para poder romperse, si es necesario por la ejecución de la ley.

4. Internet relacionó crimen (tradicional)

Muchos antecedentes - en Internet están relacionados con la publicación indeseable (o copiando). Los antecedentes - conexos, crímenes tales como pornografía infantil, las violaciones de propiedad y racismo tienen ese aspecto en común.

4.1 Línea de emergencia contra la pornografía infantil

El NLIP, la sociedad al que la mayoría de los proveedores de Internet en Países Bajos pertenecen, crearon en Internet de línea de emergencia contra la pornografía infantil a mediados de 1996. Los policías crearon este centro desde una fase temprana y participó activamente CRIS, Crimen y Tecnología de Información. Desde hace mucho, los contactos han existido con el XS4ALL, y los proveedores de Internet en Amsterdam apoyan la línea de emergencia.

Aunque la línea de emergencia signifique para una supresión más efectiva y eficiente en la pornografía infantil sobre Internet, una evaluación realizada por el CRI mostró que hay razones para dudar su eficacia.

La creación de la línea de emergencia ha limitado el efecto sobre la corriente de pornografía infantil disponible sobre Internet en los Países Bajos. La razón es que la línea de emergencia puede actuar sólo si la fuente se conoce y si la fuente está en los Países Bajos.

Aunque la línea de emergencia Internet es contra fines de pornografía infantil no incluye la acción de tomar acciones de pornografía originados en otros

países, la línea de emergencia ha pasado 7 informes a los policías. En el futuro próximo, el procedimiento con respecto a informes extranjeros será modificado.

En un número de causas en otros países, particularmente Japón, la pornografía infantil se distribuyó sobre Internet y el autor reclamó que estas era permisible según normas locales.

Además, la regulación propia en el supuesto del incumplimiento se limita. Se requiere un mecanismo que habilite la acción desde las autoridades, con la acción criminal, terminando el factor en una serie de medidas para suprimir la distribución de pornografía infantil sobre Internet.

También, en los Países Bajos, los desarrollos en el sector de negocio en Bretaña, en la consulta con DTI y los policías en el R3 Safetynet y otros desarrollos internacionales (p. ej. PICS - Andén para Internet la Selección Contenta) se siguen estrechamente.

4.2 Línea de emergencia Internet contra el racismo

Próxima a la línea de emergencia contra la pornografía infantil, existe una línea de emergencia contra publicaciones racistas en Internet que se estableció en Febrero 1997 por la Organización Nacional Antiracismo.

4.3 Nuevos tipos de Internet

Los siguiente son algunos ejemplos recientes de nuevos tipos de líneas de crimen en los Países Bajos.

Los criminales en línea - En Abril de este año, los seguidores de fútbol del PSV hicieron una invitación de lucha por medio de Internet a los seguidores del Ayax. La invitación se transmitió mediante dos proveedores de Internet Holandeses. Las autoridades de justicia han demandado que los proveedores revelen la identidad de los autores, pero de ninguna manera es seguro que ellos lo conseguirán. Alguien puede pasar como si fuera otra persona y todavía ser apto para distribuir mensajes incitando a la violencia. Hay numerosas maneras para permanecer anónimo sobre Internet, a expensas de otras personas.

Pero también, los individuos más astutos que desean distribuir mensajes discutibles (requiriendo violencia, publicando pornografía infantil, o textos racistas) y publicación de casinos ilegales no están bajo la legislación Holandesa.

Internet se usa también para distribuir cuadros muy horribles y mórbidos en la forma digital de gente siendo asesinado. Estas imágenes no son punibles en los Países Bajos, a menos que la Corte decida de otra manera cuando se distribuye a los niños menores de 16 años.

Con el avance de las tecnologías, hay muchas posibilidades por parte de un individuo para componer imágenes con el contenido que no puede distinguirse de la realidad..

También, las nuevas acciones de pago mediante Internet pueden conducir a propósitos criminales, incluyendo el dinero negro.

Otros crímenes de Internet que son probables son:

- juego por Internet, frecuentemente usando encriptación

- el uso terrorista de Internet.

Aparte de la amenaza física, hay la amenaza virtual.

4.4 Uso ilegal de las nuevas tecnologías en los Países Bajos

El uso ilegal de las nuevas tecnologías encontrado en los Países Bajos ha sido el siguiente:

- el uso de técnicas de observación (sonando fuera)
- la interceptación de e-mail mensajes
- el taxi de computadoras con Internet en conexión
- la interceptación y derivación de semáforos
- la derivación de buzones conectó a ATF y GSM de redes
- el abuso de la cajetilla que transmite (desde la prisión)
- el abuso de *21
- derivación de nº tarjeta para llamar a centros mediante cajas de teléfono
- el trazado de ALFILER codifica mediante la llave H (repite)

4.5 Remarcado procesadores Intel SYMBOL 210 \f "Symbol" \s 12

Otro problema es el remarcado existente de los procesadores Intel Pentium. (Como es conocido existe un no autorizado remarcado de procesadores

Intel con identificadores incorrectos). El caso más reciente se basa en el remarcado de procesadores Pentium 100 Mhz. a partes de procesadores Pentium 166 Mhz. Para este proceso fueron utilizados equipos muy caros y complejos.

4.6 Comercio ilegal de tarjetas SIM

El comercio ilegal de tarjetas SIM es una de las asignaturas del mercado. En la competición para obtener una participación en el mercado (en Países Bajos, un teléfono portable es frecuentemente más barato que una hogaza de pan), las compañías frecuentemente fracasan para introducir medidas debidas de seguridad. Muchos talleres de teléfono aceptan una fotocopia de un pasaporte o conducir la licencia que el futuro cliente ha traído por sí mismo.

Los teléfonos de bolsillo proveen a los criminales con una oportunidad de hacer negocio lucrativo. Obviamente, cuando una demanda llega a los policías, los números en cuestión se bloquean, pero los teléfonos en sí mismos se venden en otros países Europeos, parejos sin un SIM de tarjeta. En estos países, los clientes no son tentados con los teléfonos libres de bolsillo, pero ellos se venden por centenares de florines. Aquí, las subscripciones se toman sin un teléfono; luego tal teléfono se comprará sobre el mercado negro.

4.7 Pre-pago tarjetas de teléfono

Otro desarrollo que ocasiona preocupación a las autoridades, es el uso creciente de (pre-pago) tarjetas de teléfono, modelos que hacen una visita aun más anónima del que usó para ser. En la mayoría de los países Europeos, en conformidad con el reglamento de intimidad, las tarjetas y sus usuarios no son registrados.

5. Cooperación Internacional (policías)

Como nosotros hemos oído muchas veces esta consulta, Internet - el conexo crimen es el crimen fronterizo de cruz, que hace necesaria la cooperación internacional. El enfoque al crimen de computadora es diferente para cada país, los métodos de enjuiciamiento y la investigación que se usan pueden ser similares.

La cooperación global se necesita exitosamente para luchar pelear contra el crimen. Debe ser posible pedir asistencia en un país aún cuando el crimen no haya tenido lugar allí. Una lucha efectiva contra el crimen de computadora depende de

dos de condiciones: co-operación entre países y una preparación para engranar legislación nacional y adaptar lo a las nuevas posibilidades digitales.

5.1 Interpol de grupo de trabajo sobre el Crimen y Tecnología de Información

A nivel internacional, el grupo de trabajo Interpol sobre el Crimen y Tecnología de la Información intenta fomentar a nivel internacional la estandarización de métodos, procedimientos y armonizar la legislación. Como nosotros hemos recibido noticias de Phil Swinburne.

Otra importante organización a nivel internacional en la lucha de crimen de computadora es la organización internacional de la Evidencia de Computadora (IOCE).

5.2 Presidencia holandesa de la Unión Europea

La presidencia Holandesa ha alegado la necesidad de hacer un inventario de las actividades emprendidas con respecto a Internet. A tal fin, el Partido De trabajo sobre el Contenido Ilegal y Nocivo sobre el Internet se ha establecido bajo la presidencia de la Comisión Europea, como dijo ayer Mr. Berend de Ene Drijber.

La Conclusión

Mis conclusiones son muy breves.

En mi opinión: Cualquier ley estará sin el efecto práctico si un injuriador no puede hacerse responsable.

Muchas gracias