La Cooperación Policial Internacional en el Ciberespacio

NICOLA DI LEONE

Representante de la Policía Italiana

SLIDE 1

In advance, italian delegation want to thank the Guardia Civil for the invitation and to have given us the possibility to partecipate and to do a presentation in this conference. We have appreciated very much the hospitality and the availibility of the organizators which has been wonderful.

SLIDE 2

We are Computer Crime unit which is composed by 30 specialised investigators coming from different offices of italian police department. Each of us have, besides the computer crime specialization, a special experience in investigation in other fields like: organized crime, terrorism, economic crime and so on.

SLIDE 3

At the same time, we coordinate the computer crime squads all of Italy, when the investigation is in progress.

SLIDE 4

As you can see, the duties of the N.O.P.T. are:

• to investigate on computer crime (or to fight each crime connected to the telecommunications)

• to locate new investigation tecniques during the case in progress

to build up databases to improve our background, to gather information, to study the criminal profiles of the guilties and to make an efficient plans for the future investigation.

SLIDE 5

•To take care of the up-to-date of the specialised investigators

• To take care of the teaching and the specializing of the computer crime squads all of Italy

SLIDE 6

•Inspections

• Search warrants

• Seizures

• Telephone wiretapping

Data-communication wiretapping

SLIDE 7

Even if with a delay with respect to other more developed countries, Italy has started to record a quite high increase in the computerization of public and private sectors, as well as in the expansion of computer networks. However, we have observed that computer crime increases on a daily basis, both at the quantitative and qualitative level. The development of a more and more advanced technology has caused the coming up of some criminal kinds of behaviour that were unknown in the past. Moreover, it provides ever more efficient equipment for the perpetration of traditional offences. For this reason, we can say that computer crime risks to be the "server" of the traditional criminal network. It is necessary to take into serious consideration these new kinds of illegal behaviour, because they could be the cause of a standstill in the technological development itself. In Italy, we have identified many reasons of concern on the ground of our past experiences.

SLIDE 8

These concernes are due to the nature of the phenomenon itself, because the number of offences such as computer frauds, computer piracy and the well known software piracy are increasing constantly. In many countries, "computer frauds" are considered responsible for the most serious economic damages.

SLIDE 9

Nowadays, computer pirates have a wider range of action. By now, public and private offices, residences and public services are full of computer that are often connected to a network and among each other. The Internet world web, then, has determined a very revolution in the world of computer technology. Therefore, security issues and updating of investigative techniques are growing in importance, surprisingly.

SLIDE 10

Still now, not only among hackers' parents, but also in judicial environments is heard saying how good these young computer experts are, who succeed in breaking others' data banks; these are boyish pranks; that security is a problem of network and database managers, and, therefore, if they are not able to protect their systems, it is not fault of those "poor geniouses". Not only is this believe widespread among common, generally unskilled people, but often among magistrates and law enforcement agencies, too. Many times I was said by my colleagues "lucky you, they let you play all day with computers and pay you for that!". Hence, the awareness about the unlawful nature of these kinds of behaviour is rejected above all at the cultural level.

SLIDE 11

Even if in Italy there are laws with reference to computer crime and software piracy since 1994, the number of reports to law enforcement agencies and judicial authorities is ridiculous for two main reasons:

- generally the person who detects an illegal access to a system is the system manager ; we can say "the father of the system". It is clear that after making the company spends hundreds of thousands of dollars for security, it is not happy to report that the system has been breaked, actually by a boy with a personal computer and a modem: actually, the costs of the equipment isn't so expensive, like in the past.

- companies and banks in particular believe that by denouncing the intrusion, the losses in their image would be more serious than economic damages.

SLIDE 12

As surfaced by the N.O.P.T. investigators, in Italy computer systems are still protected in a ridiculous way, because in main cases, common words abound, as well as names and dates, can be easily discovered by a simple software within few minutes, as we all know.

SLIDE 13

The principal elements of a computer security system are:

- hardware
- software
- kinds of behaviour.

Taking into consideration these three elements, I can assert today that, despite the ever increasing dependance of entire economy branches on computer, awareness in security matters is still lacking: we pass from one excess to the other, from psychological terrorism to absolute indifference. In this scenario, reports to the police range from "0" downwards: try to count them!

SLIDE 14

Jurists, sociologists, and security experts define computer crime in different ways.

Many countries resort to the idea of "computer fraud"; in others, the use of a computer as a means characterizes the offence. In Italy, there is a proper law with respect to computer-related crimes.

SLIDE 15

There are, then, traditional offences committed with the help of computer technology. For example, the production of counterfeited bank-notes is not a computer crime. If, however, the techniques adopted are all computerized, as presently occur, this offence is considered as computer related. Investigation methodologies, too, have to be adjusted to specific sectors (extortions, loan-sharking, etc.)

SLIDE 16

Now that computer-related offences have been identified, it is possible to distinguish their different level of dangerousness. In Italy, for methodology reasons deriving from investigative needs, we have made distinctions in the level of dangerousness according to the kind of criminal involved. More on the grounds of our experience rather than on the scanty statistic data available, because the actual number of offences remains unknown for lack of reports to the police, the scale of dangerousness can be described as follows:

- insiders
- organized crime (increasing phenomenon)
- external hackers, (who become more and more dangerous due to the expansion of the computer web).

SLIDE 17
Traditional crime
Organized crime

SLIDE 18
Traditional criminality and economic criminality are specialized in the field of computer frauds or in hardware smuggling and counterfeiting.

We already had in the past big italian industries who referred their worry for these kinds of criminals, who have the capacity to create and to build similar equipments, otherwise more powered than the original sold in legal trade. It is an enormous trade which can gain to the criminality a lot of money.

Actually, the traditional criminality is replacing the old methods of communications with the new tecnique to spread the illegal material through Internet. For example, the spreading of child pornography.

SLIDE 19
The organized crime often use the data-networks to comunicate and to exchange information with other criminal users. The organized crime use the data-equipment to manage criminal activities, like the extorsions, loan-sharking, money-laundering and so on.

SLIDE 20
Who are the actors of this criminal scenario?

It isn't easy to answer at this question. If we want to investigate in computer crime, first of all, we have to classified the categories of the criminals because they are different of each other and their goals are different.

SLIDE 21

Most of all, the main category of computer pirate are the unfaithfull employees.

SLIDE 22

The another category are the Phreakers. They are the scrounger of the datanetwork because they exploit telephone and computer lines causing others to pay for their calls. It could say that is a "sport activities" for them, but I don't want to offence anybody who plays " real sports activities".

SLIDE 23

When we speak about The hackers, like a person who comes from outside of the system, we have to distinguish, because today the profile of hacker is complex. In fact, we are speaking about a person who is, in the average, 13-28 years old, because he is able to dedicate many time at his activity in front of computer. After 25/28 years the percentage of hackers decrease because there other interests (family, work and so on)

SLIDE 24

The first characteristic of the hackers, in fact, is that they are able to dedicate many time to connect in Internet, to try new tecniques and gather information about the hacking of the system.

SLIDE 25

As the Philosophy is the spreading of information of their "successful", the result of their activities can teach to other "hackers beginners".

SLIDE 26

The Internet sites or Bulettin Board Ssystems are the sites where is possible fot the hackers to exchange illegal information gathered during their activities. These Information concernes the entences in the slide.

SLIDE 27

In the various typology of computer pirate which we met in our experience, we can catalogate the main profile of them, but we haven't to forget that the phenomenon is going to change.

SLIDE 28

Through the variuos categories of hackers, we can individuate a cathegory of them which conduct a professional illegal activities, they are the spies, for industrial espionage, and the viruses writers.

SLIDE 29

The italian reality gave to N.O.P.T. investigators a various criminal scenario for the profiles of hackers: the so-called cultural of criminal extremist organization, the estabilishment of currency of thinking (animalist, ambientalist), or particular criminal organizations (like satan sects or other fanatic people) which use modern tecnologies.

Actually, in Italy, the politic activists spread information and their political thinking through the datanetwork. In particular they created various specific Internet nodes to make easy the diffusion of political information. These kind of behaviour can cause problem if there isn't an efficient control of police forces, because the datanetwork can be used also to act illegal goals. The same activities was conducted, in the past, through the use of the leaflets.

SLIDE 31

In this operation we discover a person who violated the computer system of tranplant center of organs of University of medicine in Rome. This computer system provide to regulate the list of the patients who are waiting to submit a tranplant organs.

SLIDE 32

In this operation we smantled a criminal organization who wanted to perpetrate a big fraud against the Automatic Teller Service. They made several numbers of false cards to withdraw money from Automatic Teller Machine.

SLIDE 33

In this operation we smantled an organization who spreaded passwords for Videotel Communications stolen from the legal owners.

SLIDE 34

In this operation we located a prson who provide to disseminate floppy disk concerning A.I.D.S. information, but infected by viruses, to extort money from the infected computer owners.

SLIDE 35

In this operation we discover a person who build up a trade in child pornography, between Italy and american Bulletin Board Systems.

SLIDE 36

In this operation we discovered a person who perpetratd a fraud to a bank through the money transfers via computer.

SLIDE 37

In this operation we smatled a criminal organization addicted to perpetrate several kinds of computer crimes (hacking, dissemination of logins, passwords, cloning of cellular phones, phreaking, credit cards fraud).

La Cooperación Policial Internacional en el Ciberespacio*

NICOLA DI LEONE

Representante de la Policía Italiana

DIAPOSITIVA 1

Antes de nada, la delegación italiana quiere agradecer a la Guardia Civil la invitación y por darnos la posibilidad de participar y hacer una presentación. Nosotros hemos apreciado mucho la hospitalidad y la organización de este evento, que ha sido maravillosa.

DIAPOSITIVA 2

Nosotros somos una unidad de Delitos Informáticos que está compuesta por 30 investigadores especializados que vienen desde oficinas de diferentes departamentos de policías italianos. Cada uno de nosotros tiene, aparte de la especialización de delitos informáticos, una experiencia especial en la investigación en otros campos como: el crimen organizado, terrorismo, crimen económico y otros.

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

DIAPOSITIVA 3

A la vez, nosotros coordinamos los batallones de delitos informáticos de toda Italia, cuando la investigación está en curso.

DIAPOSITIVA 4

Como pueden ver, los deberes de la N.OP.T. son:

- investigar sobre el delitos informáticos (luchar en cada caso con los adelantos en telecomunicaciones)
- ubicar nuevas técnicas de investigación durante la causa en curso.
- construir las mejores bases de datos para mejorar nuestros antecedentes, para reunir informes, para estudiar los perfiles criminales de los convictos y para hacer unos planos eficientes para la futura investigación.

DIAPOSITIVA 5

- tener cuidado y estar al día de los investigadores especializados
- tener cuidado del magisterio y la especialización de los batallones de delitos informáticos de toda Italia

DIAPOSITIVA 6

- Las Inspecciones
- Los Mandamientos de registro
- Los Embargos
- Comunicaciones telefónicas. Transmisión de datos.

DIAPOSITIVA 7

Aún cuando con demora con el respecto a otros países más desarrollados, Italia ha comenzado a inscribir un aumento bastante alto en la informatización pública y de sectores privados, así como también en la expansión de redes de computadoras. Sin embargo, nosotros hemos observado que esos delitos informáticos aumenta diariamente, ambos al nivel cuantitativo y cualitativo. El desarrollo de una tecnología más avanzada ha causado y surgido de algunos tipos criminales de comportamiento que eran desconocidos en el pasado. Además,

proveen equipamiento siempre más eficiente. Es necesario tomar en seria consideración estos nuevos tipos de comportamiento ilegal, porque ellos podrían ser la causa de una inmovilización en el desarrollo tecnológico en sí mismo. En Italia, nosotros hemos identificado muchas razones de interés sobre el terreno de nuestras experiencias pasadas.

DIAPOSITIVA 8

Estos intereses están debido a la naturaleza del fenómeno en sí mismo, porque el número de crímenes tales como fraudes de computadora, piratería de computadora y la piratería bien conocida de software aumentan constantemente. En muchos países, "los fraudes de computadora" se consideran responsables por los daños económicos más serios.

DIAPOSITIVA 9

Hoy día, los piratas de computadora tienen una gama más amplia de acción. Por ahora, a nivel público y oficinas privadas, residencias y servicios públicos están lleno de computadoras y que se conectan frecuentemente a una red entre el uno y el otro. Internet, la tela mundial, entonces, ha determinado una misma revolución en el mundo de tecnología de computadora. Por lo tanto, las emisiones de seguridad y actualización de técnicas investigadoras crecen en la importancia, sorprendentemente.

DIAPOSITIVA 10

Todavía ahora, y no solamente entre hackers padres, también en ambientes judiciales se escucha lo bueno que son estos jóvenes peritos de computadora, quienes pueden hacer quebrar otros bancos de datos; esta seguridad es un problema de administradores de base de datos y de red, y, por lo tanto, si ellos no son aptos para proteger sus sistemas, no es un problema de esos "pobres genios". Esto no está generalizado entre gente común, gente generalmente inexperta, pero demasiado frecuentemente entre agencias de ejecución de la ley y magistrados. De aquí en adelante, la conciencia sobre la naturaleza ilegal de estos tipos de comportamiento se rechaza sobre todo al nivel cultural.

DIAPOSITIVA 11

Aún cuando en Italia hay leyes con referencia al software y delitos informáticos de piratería desde 1994, el número de informes a agencias de

ejecución de la ley y las autoridades judiciales es ridícula por dos razones principales:

- generalmente la persona quien detecta un acceso ilegal al sistema es el administrador de sistema; nosotros podemos llamarlo "el padre del sistema". Es claro que la compañía gasta centenares de millares de dólares para la seguridad, no es agradable informar que el sistema se ha roto, realmente por un muchacho con una computadora personal y un modem: actualmente, los costos del equipamiento no son tan caros, como en el pasado.

- las compañías y los bancos en particular creen que por desahuciar la intrusión, las pérdidas en su imagen serían más serias que los daños económicos.

DIAPOSITIVA 12

Como observación de los investigadores de la N.O.P.T., los sistemas de computadora de Italia se protegen todavía en una manera ridícula, porque en las causas principales, las palabras comunes abundan, así como también nombre y fechas, pueden ser fácilmente descubiertos por un software simple dentro de pocos minutos, como todos saben.

DIAPOSITIVA 13

Los elementos mayores de un sistema de seguridad de computadora son:

- hardware
- software
- tipo de uso o comportamiento.

Debemos tomar en consideración estos tres de elementos, puedo afirmar hoy que, a pesar del aumento constante de la dependencia que la economía entera ramifica sobre la computadora, la conciencia en las materias de seguridad todavía es escasa: nosotros pasamos desde una demasía al otro, desde el terrorismo psicológico al despego absoluto. En este escenario, los informes policiales oscilan desde "0" lo más abajo: intenten contarlos!

DIAPOSITIVA 14

Los juristas, sociólogos, y los peritos de seguridad definen los delitos informáticos en maneras diferentes.

Muchos países recurren a la idea de "fraude de computadora"; en otros, el uso de la computadora está caracterizado por los delitos. En Italia, hay una ley relacionada con respecto a la computadora y sus delitos.

DIAPOSITIVA 15

Hay, entonces, delitos cometidos con la ayuda de tecnología de computadora. Por ejemplo, la producción de notas de bancos falsificados no es un delito informático. Sin embargo, las técnicas adoptadas son todas computerizadas actualmente, estos delitos se consideran como relacionados con la computadora. Las metodologías de investigación, a menudo, tienen que ser ajustadas a sectores específicos (extorsiones, etc.)

DIAPOSITIVA 16

Ahora en esa computadora ya identificada, es posible distinguir su nivel diferente de peligrosidad. En Italia, por razones de metodología que se derivan de necesidades investigadoras, nosotros hemos hecho distinciones en el nivel de peligrosidad según el tipo de criminal implicado. Más sobre los terrenos de nuestra experiencia que sobre antecedentes estadísticos escasos y disponibles, porque el número real de ataques es desconocido por la falta de informes a los policías, la escala de peligrosidad puede describirse como se indica a continuación:

- Internos
- Crimen organizado (fenómeno creciente)
- Externo (hackers, que llegan a ser más y más peligrosos debido a la expansión de la WEB).

DIAPOSITIVA 17

El crimen tradicional

El crimen organizado

DIAPOSITIVA 18

La criminalidad tradicional y la criminalidad económica se especializan en el campo de los fraudes de computadora o en el crimen informático contrabandeando y falsificando.

Nosotros ya tuvimos en las industrias italianas una gran preocupación por estos tipos de criminales, la competencia tiene equipación para crear y para construir equipamientos similares, de otra manera más potentes que el original vendido en el comercio legal. Es un comercio enorme que puede ganar en la criminalidad mucho dinero.

Realmente, la criminalidad tradicional reemplaza los métodos viejos de comunicaciones con el nuevo procedimiento para esparcir el material ilegal mediante Internet. Por ejemplo, la expansión de pornografía infantil.

DIAPOSITIVA 19

El crimen organizado frecuentemente usa los antecedentes - redes de comunicaciones - cambiando informes con otros usuarios criminales. El crimen organizado usa antecedentes y buen equipamiento para administrar actividades criminales, como las extorsiones, sharking, blanqueando el dinero.

DIAPOSITIVA 20

¿ Quienes son los actores de este escenario criminal?

No es fácil de contestar a esta preguntas. Si nosotros queremos investigar delitos informáticos, ante todo, nosotros tenemos que clasificar las categorías de los criminales porque ellos son diferentes del uno al otro y sus metas son diferentes.

DIAPOSITIVA 21

La mayoría de todos, la categoría principal de pirata de computadora son los empleados.

DIAPOSITIVA 22

La otra categoría son el Phreakers. Ellos son el como sablista de la datanetwork porque ellos con la computadora y líneas de teléfono pueden hacer pagar a otros sus llamadas. Podría decir que es un "actividades deportivas" para ellos, pero no quiero ofender a nadie que realice "actividades deportivas reales".

DIAPOSITIVA 23

Cuando nosotros hablamos de hackers, es una persona que viene de fuera del sistema, nosotros tenemos que distinguir, porque hoy el perfil es complejo. De hecho, nosotros hablamos de una persona en el promedio, 13-28 años de edad, apto a dedicar mucho tiempo a su actividad al frente de computadora. Después de 25/28 años como el porcentaje de hackers enmayor disminución porque hay otros intereses (la familia, trabajo ...)

DIAPOSITIVA 24

La característica primera del hacker, de hecho, es que ellos son aptos para dedicar mucho tiempo a conectar en Internet, para tratar nuevas tecnicas y reunir informes sobre el sistema.

DIAPOSITIVA 25

Como la Filosofía es la expansión de informes de su "exitoso proyecto", el resultado de sus actividades puede enseñar otros "hackers principiantes".

DIAPOSITIVA 26

Los WEB Sites o Boletines Electrónicos son los sitios dónde hay posibles informes de las actividades de los hackers.

DIAPOSITIVA 27

Entre los diversos tipos de pirata de computadora que nosotros encontramos en nuestra experiencia, podemos catalogar el perfil principal de ellos, pero nosotros no tenemos para olvidar que el fenómeno puede cambiar.

DIAPOSITIVA 28

Mediante las categorías de hackers, podemos especificar una categoría de ellos que conduce unas actividades ilegales profesionales, ellos son los espías, para el espionaje industrial, y los creadores de virus.

DIAPOSITIVA 29

La realidad italiana dió a los investigadores de N.O.P.T. un diverso escenario criminal para los perfiles de hackers: la tan -llamado cultural de organización criminal extremista u organizaciones criminales particulares (como sectas de satán o la otra gente fanática) que usa modernas tecnologias.

Realmente, en Italia, los activistas de política esparcen informes y mediante el datanetwork. En particular ellos crearon en Internet un específico nódulo para hacer fácil la difusión de informes políticos. Este tipo de comportamiento puede causar problemas si no hay un control eficiente en los cuerpos de policía, porque las datanetwork puede usarse también para actuar metas ilegales. Las mismas actividades se condujo, en el pasado, mediante el uso de los folletos.

DIAPOSITIVA 31

En esta operación nosotros descubrimos una persona quien infringió el sistema de computadora del centro tranplante de órganos de la Universidad de Medicina en Roma. Este sistema de computadora provee para regular la lista de los pacientes que espera para someter unos tranplantes de órganos.

DIAPOSITIVA 32

En esta operación nosotros desmantelamos una organización criminal quien quiso perpetrar un fraude grande contra el Servicio Automático de

Cajero. Ellos hicieron varios números de tarjetas falsas para retirar dinero de la Máquina Automática de Cajero.

DIAPOSITIVA 33

En esta operación nosotros desmantelamos una organización quien esparció contraseñas para Videotel de Comunicaciones hurtadas desde los propietarios en derecho.

DIAPOSITIVA 34

En esta operación nosotros ubicamos un personas que proveían para diseminar discos flexibles en lo que concierne a A.I.D.S. el informe, pero infectado por virus, para extorsionar dinero desde los propietarios infectos de computadora.

DIAPOSITIVA 35

En esta operación nosotros descubrimos una persona quien construye un comercio en la pornografía infantil, entre Italia y América mediante Sistemas de tablero de anuncios.

DIAPOSITIVA 36

En esta operación nosotros descubrimos una persona quien perpetraba un fraude al banco mediante los giros de dinero por medio de la computadora.

DIAPOSITIVA 37

En esta operación nosotros desmantelamosuna organización criminal que envició a perpetrar varios tipos de crímenes de computadora (diseminación de logins, contraseñas, cloning de teléfonos celulares, phreaking, fraude de tarjetas de crédito).