FUNDAÇÃO DE ENSINO "EURÍPIDES SOARES DA ROCHA"
CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA - UNIVEM
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

TIAGO BRACCIALLI

CLASSIFICAÇÃO DE ATAQUES PELA INTERNET E PROPOSTA DE UM AMBIENTE ANTI-CRIME

MARÍLIA
2005

TIAGO BRACCIALLI

CLASSIFICAÇÃO DE ATAQUES PELA INTERNET E PROPOSTA DE UM AMBIENTE ANTI-CRIME

Trabalho de Conclusão de Curso apresentado ao Curso de Ciência da Computação da Fundação de Ensino Eurípides Soares da Rocha, Mantenedora do Centro Universitário Eurípides de Marília - UNIVEM, como requisito para obtenção do grau de Bacharel em Ciência da Computação.

Orientador:
Prof. Dr. Marcos Luiz Mucheroni

MARÍLIA
2005

BRACCIALLI, Tiago
Classificação de ataques pela internet e proposta de um ambiente Anti-Crime / Tiago Braccialli; orientador: Marcos Luiz Mucheroni. Marilia, SP: [s.n.], 2005.
94 f.

Monografia (Bacharelado em Ciência da Computação) — Centro Universitário Eurípides de Marília – Fundação de Ensino Eurípides Soares da Rocha.

1. Cibercrimes 2. Crimes Virtuais
CDD: 004.0285

TIAGO BRACCIALLI

CLASSIFICAÇÃO DE ATAQUES PELA INTERNET E PROPOSTA DE UM AMBIENTE ANTI-CRIME

Banca examinadora da monografia apresentada ao Curso de Ciência da Computação da Fundação de Ensino Eurípides Soares da Rocha, Mantenedora do Centro Universitário Eurípides de Marília - UNIVEM, para obtenção do grau de Bacharel em Ciência da Computação.

Resultado: _____

ORIENTADOR: Prof. Dr. Marcos Luiz Mucheroni

1º EXAMINADOR:_____

2º EXAMINADOR:_____

Marília, ...de .... de 2005.

DEDICATÓRIA

Dedico este trabalho à minha mãe, que além de me apoiar sempre foi um grande exemplo de determinação, dedicação e boa vontade e também à minha namorada por sempre me trazer calma e forças para dar um passo a mais para a conclusão deste trabalho.

AGRADECIMENTOS

Gostaria de agradecer primeiramente ao meu Orientador, prof. Dr. Marcos Luiz Mucheroni por ter tido sempre paciência comigo, me orientado, me ouvido e ajudado e por ter sido mais do que um orientador, ter sido um professor e amigo. Queria agradecer também à banca avaliadora parcial a qual contribuiu com seus pensamentos e idéias para o melhor desenvolvimento deste trabalho e também agradecer a banca avaliadora final que com muita paciência lerá este trabalho e estará presente para me auxiliar a encontrar um melhor caminho para eu continuar minhas pesquisas e aprendizado. Por fim gostaria de agradecer a todos os outros que de alguma maneira ajudaram para a conclusão deste trabalho.

Apenas duas coisas são infinitas: o universo e a estupidez humana. E eu não tenho certeza se isso é verdadeiro para o primeiro (Albert Einstein)

BRACCIALLI, Tiago. **Classificação de ataques pela internet e proposta de um ambiente Anti-Crime**. 2005. 94 f. Monografia (Bacharelado em Ciência da Computação) - Centro Universitário Eurípides de Marília, Fundação de Ensino Eurípides Soares da Rocha, Marília, 2005.

RESUMO

Este trabalho teve por objetivo discutir as questões legais e éticas de crimes virtuais, tanto quanto apontar os principais tipos de crimes e ataques na Internet e propor um ambiente preventivo. Para a realização do estudo foi realizado o levantamento bibliográfico dos principais textos da área que resultou na análise do conteúdo específico de cibercrimes e a fundamentação do conhecimento para elaboração de proposta de software de detecção e prevenção deste tipo de delito. Após esta etapa foi implementada a proposta de um ambiente preventivo, que resultou na proposta de uma ferramenta de auxílio para combater estes cibercrimes.

Palavras-chaves: cibercrimes; crimes virtuais

BRACCIALLI, Tiago. **Classification of attacks for the InterNet and proposal of a Anti-Crime environment**. 2005. 63 f. Monografia (Bacharelado em Ciência da Computação) - Centro Universitário Eurípides de Marília, Fundação de Ensino Eurípides Soares da Rocha, Marília, 2005.

ABSTRACT

This work had for objective to argue the legal and ethical questions of virtual crimes, as much how much to point the main types of crimes and attacks in the InterNet and to propose a preventive environment. For the accomplishment of the study it was carried through the bibliographical survey of the main texts of the area that resulted in the analysis of the specific content of cybercrimes and the recital of the knowledge for elaboration of proposal of software of detention and prevention of this type of delict. After this stage was implemented the proposal of a preventive environment, that resulted in the proposal of an aid tool to fight these cybercrimes.

Keywords: cybercrimes; virtual crimes

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CERT - Centro de Estudos, Resposta e Tratamento de incidentes de segurança no Brasil

CAIS - Centro de Atendimento a Incidentes de Segurança

DOS - Deny of System

dDOS – Distributed Deny of System

PC - Pessoal Computer(Computador Pessoal)

SUMÁRIO

INTRODUÇÃO

Com a popularização da computação, sem a formação e uma cultura adequada para delimitar e cercear crimes cometidos usando a internet, muitas pessoas e instituições foram vítimas inocentes de diversas formas de crimes cometidos com uso do computador: saques com uso de senhas, destruição de dados, divulgação de pornografia ou difamação, etc.

Nos dias de hoje já existe uma maior divulgação dos diversos tipos de crimes virtuais e dos danos causados por estes. A imprensa tem desempenhado um papel importante e efetivo neste aspecto e também tem tentado conscientizar a população sobre os perigos e as medidas preventivas, devido ao crescente aumento nesses tipos de crimes.

Tendo em vista que boa parte da população brasileira já tem algum acesso a Internet, seja acesso direto, ou acesso a e-mail por *lan house*, existe a necessidade de realizar projetos de conscientização para que ela não seja prejudicada por pessoas com intenções ruins. As pessoas com má intenção podem agir de duas maneiras: 1) utilizam a máquina do usuário para cometer outros crimes ou 2) utilizam os dados do usuário, para roubar informações, como senhas bancárias e de cartão de crédito.

Apesar de nos dias de hoje muitos dos crimes virtuais estarem sendo punidos com base na legislação vigente, ainda existem muitos outros tipos de crimes que ficam sem uma punição adequada por não ter respaldo no código penal brasileiro vigente.

O fato, também, de o que pode ser considerado uma prova concreta num crime virtual torna difícil a ação das polícias que cuidam desses tipos de crimes. Hoje em dia algumas Delegacias de Polícia já tem pessoal especializado no que se refere a crimes virtuais, com o objetivo de suprir a necessidade da população que faz ocorrência de um crime acontecido na Internet.

Por esses e outros motivos se mostra necessário realizar o levantamento dos tipos mais comuns de crimes, discutirem sobre eles e a legislação existente e propor um ambiente mais seguro de acesso à rede.

Assim, traz-se para discussão algumas questões muito citadas atualmente: Até que ponto a Internet é um beneficio? São necessários uma constituição e código penal novos para incluir-se cibercrimes, ou a constituição já enquadra isso de maneira indireta? Estamos realmente seguros? Como promover um ambiente seguro de trabalho?

Uma máxima de computação é que nenhum sistema é totalmente seguro, por isto a melhor forma e talvez a única realmente eficaz de combate aos crimes é a prevenção, e por isto, procuramos classificar os crimes e tentar classifica-los para poder, com uso de computador, preveni-los, outra forma mais ampla é educar para mudar a cultura e tornar os crimes menos freqüentes.

Este trabalho teve por objetivo discutir as questões legais e éticas de crimes virtuais, tanto quanto apontar os principais tipos de crimes e ataques na Internet e propor um ambiente preventivo.

Para realizar a prevenção através do computador adotou uma metodologia que procura usar recursos simples e baratos acessíveis a um cidadão comum.

O desenvolvimento deste trabalho deu-se por meio da análise e interpretação de dados obtidos em uma pesquisa do tipo bibliográfica e por meio da implementação de uma proposta de um software para ajudar no combate a um certo tipo de cibercrime. A pesquisa baseou-se no estudo de livros, artigos especializados, dissertações, teses e periódicos que permitiram acessar e manipular informações relevantes ao tema e fornecer subsídio teórico para a discussão.

A busca do material bibliográfico indexado deu-se pela utilização das palavras chaves: **cibercrimes, ética e crimes virtuais.**

O levantamento bibliográfico foi realizado no período entre 2000 e 2005, sendo o maior número informações correspondentes ao último ano. Utilizaram-se as seguintes fontes de pesquisa:

* Consulta a base de dados do Portal Capes e Portal UNESP;
* Biblioteca da Faculdade de Filosofia e Ciências de Marília;
* Consulta de monografias, dissertações, teses, livros e periódicos pertinentes ao tema;
* Biblioteca da UNIVEM
* Acesso on-line a sites governamentais que trabalham com a temática.

A opção por estas fontes deu-se pelo fato das mesmas possuírem catalogados os principais trabalhos pertinentes ao assunto, cibercrime, realizados nos últimos anos.

Após o levantamento bibliográfico iniciou-se o estudo do material, com o objetivo de focalizar as passagens relevantes dos textos relacionados ao trabalho em desenvolvimento.

Após esta análise realizou-se uma reflexão ampla e integradora sobre a temática estudada. Procurou-se, por fim, estabelecer um elo entre o conteúdo específico de cibercrimes e a fundamentação do conhecimento para elaboração de proposta de software de detecção e prevenção deste tipo de delito.

Inicialmente no primeiro capítulo iremos discutir sobre o conceito cibercrime e também mostrar as evidências de seu crescimento, assim como classificar os principais tipos de crimes virtuais da atualidade explicando-os.

Logo após termos conceituado cibercrime e visto a importância da discussão sobre eles, faremos uma discussão sobre as legalidades e sobre as questões éticas que envolvem um crime virtual, para assim podermos apresentar no próximo capítulo uma proposta de software que ajudará no combate a estes tipos de crimes. Assim após tudo evidenciado, discutido e

comentado concluiremos o trabalho mostrando as possibilidades futuras por base nessa pesquisa e nessa proposta de software.

1 CLASSIFICAÇÃO E TIPOS DE CIBERCRIMES

O International Data Group (2005) informou que no Brasil existem 4,9 milhões de computadores instalados no ambiente domestico. Segundo esta mesma fonte, a perspectiva é que a venda de PCs cresça 5% anualmente até 2008, e o usuário domestico é responsável por cerca de 37% de toda a venda de PCs.

Dados da United Nation Statistics Division (2005) informaram que no ano de 2002 o Brasil possuía 14.300.000 pessoas conectadas à rede. Os dados da tabela 1 mostraram que o número de usuários da Internet teve um crescimento vertiginoso no Brasil em 12 anos. Os dados desta tabela, também, mostraram que o Brasil é o país da América Latina que tem o maior número de pessoas que acessam a Internet.

Conforme pesquisa realizada pelo Ibope apud International Data Group (2005) o uso de Internet está cada vez mais disseminado no Brasil. Cerca de 26% da população brasileira têm acesso à Internet. Entre eles, 67% são de classe A e B, e o tempo que os jovens brasileiros despedem navegando pela Internet superam os dos europeus e americanos.

Estes dados sugerem que o grande número de usuários domésticos que tem acesso ao computador e à Internet, muitas vezes sem um preparo adequado poderia ser um fator desencadeador de cibercrimes.

Como se pode observar na tabela 1 o Brasil é o país da América Latina com o maior número de usuários conetados à rede mundial de computadores, a Internet, talvez por este fator o Brasil também seja visto como o país da América Latina na onde se encontra o maior foco de crimes virtuais.

Tabela 1 – Número de usuários conectados a rede na América Latina.

nternet users (ITU estimates)

Latin America & the Caribbean
Data last updated on 10 Mar 2005

Country	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003
Argentina	10000	15000	30000	50000	100000	300000	1200000	2600000	3650000	4100000	
Bahamas			2700	5000	3967	6908	11307	13130	16923	60000[1]	84000
Barbados			20	1000	2000	5000	6000	10000	15000	30000[1]	100000
Bolivia			5000	15000	35000	50000	80000	120000	180000	270000	
Brazil	40000[1]	60000[1]	170000[1]	740000[1]	1310000[1]	2500000[1]	3500000[1]	5000000[1]	8000000[1]	14300000[1]	
Chile	10000	20000	50000	100000	156875	250000	625000	2537308	3102200	3575000	4000000
Colombia		38371	68560	122500	208000	433000	664000	878000	1154000	2000113	2300202
Costa Rica	2700	9500	14500	30000	60000	100000	150000	228000	384000	800000	1200000
Cuba			10	3500	7500	25000	34800	60000	120000	160000	98000
Dominican Republic			1400	6200	12000	20000	96000	327118	397333	500000	800000
Ecuador	1800	3900	5000	10000	13000	15000	100000	180000	333000	537881	581555
El Salvador				5000	15000	25000	50000	70000	150000	300000	550000
Guatemala			300	2000	10000	50000	65000	80000	200000	400000	
Guyana				500	1000	2000	30000	50000	100000	125000	
Haiti				600		2000	6000	20000	30000	80000	150000
Honduras			2055	2500	10000	18000	35000	55000	90000	168560	272280
Jamaica		900	2700	14700	20000	50000	60000	80000	100000	600000	
Martinique						2000	5000	30000	40000	60000	80000
Mexico	25000	39000	94000	187000	595700	1222379	1822198	5058000	7410124	10032674	12250285
Panama		200	1500	6000	15000	30000	45000	90000	168690	185875	192070
Paraguay				1000	5000	10000	20000	40000	60000	100000	120000
Peru		2000	8000	60000	100000	300000	500000	800000	2000000	2400000	2850000
Puerto Rico		1000	5000	10000	50000	100000	200000	400000	600000	677000	
Suriname			500	1000	4494	7587	8715	11709	14520	20000	23000
Uruguay		2000	10000	60000	110000	230000	330000	370000	400000		
Venezuela	8800	12000	27000	56000	90000	322244	680000	820022	1152502	1274429	1549513

1 ITU estimate.

Para Turban e King (2004) ainda não existe uma definição universal para cibercrimes ou crimes cometidos por internet. Para estes autores apenas o fato da Internet ter sido utilizada como meio para a perpetrar um crime não pode classificá-lo como um cibercrime. A partir das idéias destes autores crimes tradicionais que anteriormente eram cometidos por meio de correio ou fax e atualmente são realizados pela Internet não podem ser classificados como cibercrimes, pois na maioria das jurisdições, esses crimes não são processados judicialmente como crimes de computador. Desta forma, fraude, pornografia infantil, pirataria de software e

violação de direitos autorais são crimes facilitados pelo computador, porém já existem legislações que regulamentam tais delitos. Para estes autores, seriam considerados cibercrimes a ciberinvasão e cibervandalismo.

As definições de outros autores contradizem a citada anteriormente.

Para Manzur (2000) cibercrimes são todas aquelas ações e omissões tipicas, antijuridicas e dolosas, trata-se de um eixo isolado ou de uma serie deles, cometidos contra uma pessoa fisica ou juridica, realizadas com uso de um sistema de tratamento de informação e destinada a produzir um prejuizo na vitima atraves de atentado a integridade de um sistema de informática , o qual, geralmente, produzirá de uma maneira colateral lesões a valores juridicos, e portanto, muitas vezes, um beneficio ilicito para o agente, seja ou não de carater patrimonial, atuando com ou sem obtenção de lucro.

Pinheiro (2005), a partir das idéias de Manzur (2000), definiu cibercrimes como "todos os atos ilícitos praticados através da Internet que venham a causar algum tipo de dano, seja ele patrimonial ou moral, ao ofendido".

Licks e Araújo (1994) definem como:

> a conduta que atenta imediatamente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento, armazenagem ou transmissão de dados, seja em sua forma, apenas compreendida pelos elementos que compõe um sistema de tratamento, transmissão ou armazenamento de dados, seja na sua forma compreensível pelo homem. Tal atentado deve dar-se contra os dados que, por sua vez, trabalharão sem a intervenção do homem, sendo estes o objeto material do crime.

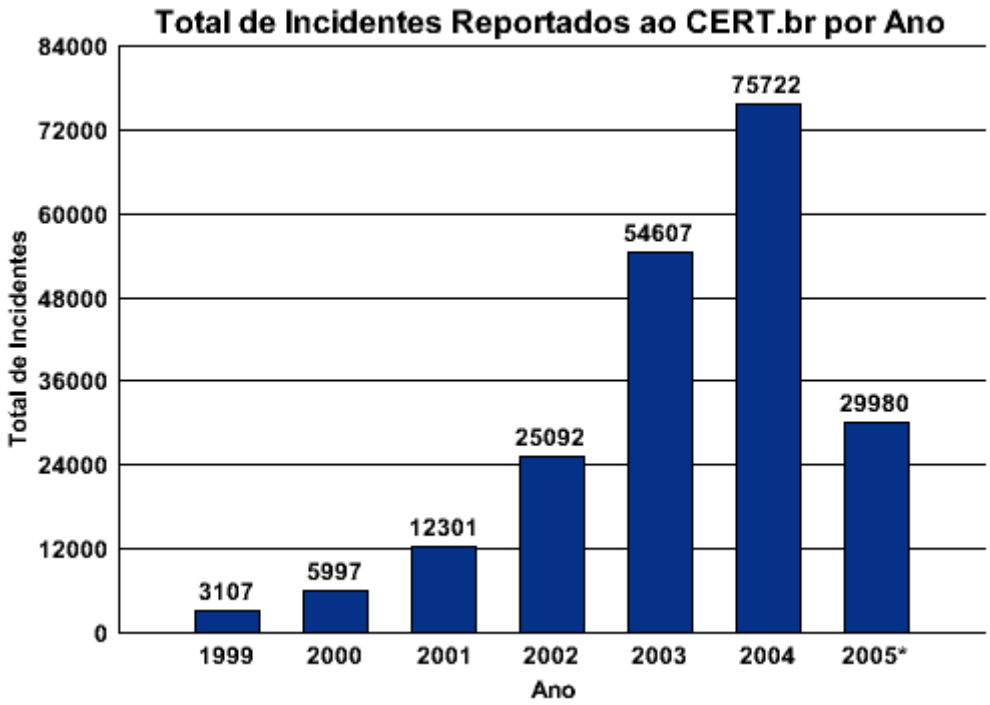
Desta forma, pode-se falar nos crimes que afetam pessoas físicas e crimes que afetam pessoas jurídicas.

1.1 Principais tipos de crimes virtuais

A Figura 1 mostrou o crescente aumento de incidentes reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT, 2005) no período entre 1999 e 2005.

O número de notificações em 1999 foi 3107 enquanto no primeiro semestre de 2005 o número de notificações atinge um total de 29980. Acredita-se que este valor pode ser maior ainda, uma vez que apenas uma parte dos crimes que acontecem são registrados. Nem todas as pessoas reportam e nem tudo que é reportado é considerado um crime. Para uma ação ser considerado crime é necessária que conste na constituição·

Valores acumulados: 1999 a junho de 2005 new



* Notificações reportadas até junho de 2005.

FIGURA 1: Dados sobre incidentes reportados ao CERT nos últimos 7 anos (Fonte: colocar na forma correta (CERT, 2005)

Os dados obtidos no Centro de Atendimento a Incidentes de Segurança - CAIS (2005) confirmaram o aumento que ocorreu nos registrados de incidentes na Internet. Segundo este Centro no mês de maio de 2005 foram realizados quase 8000 registros de incidentes na Internet (figura 2).

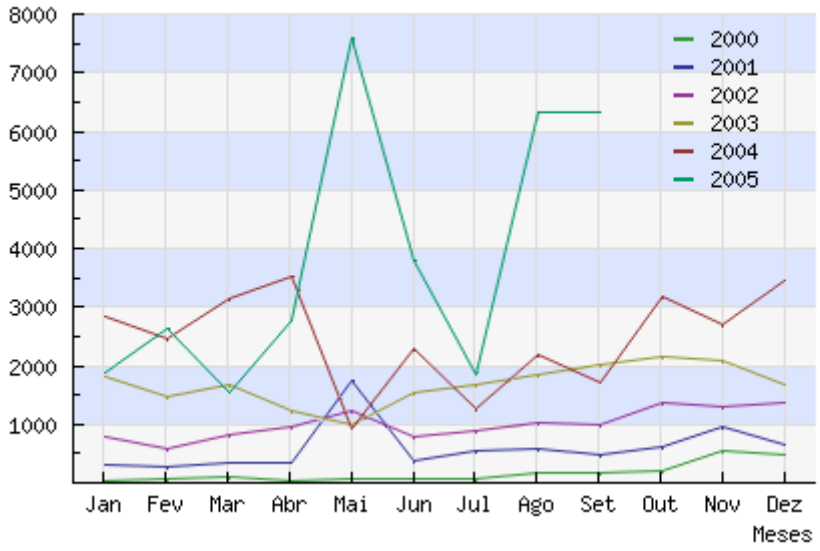
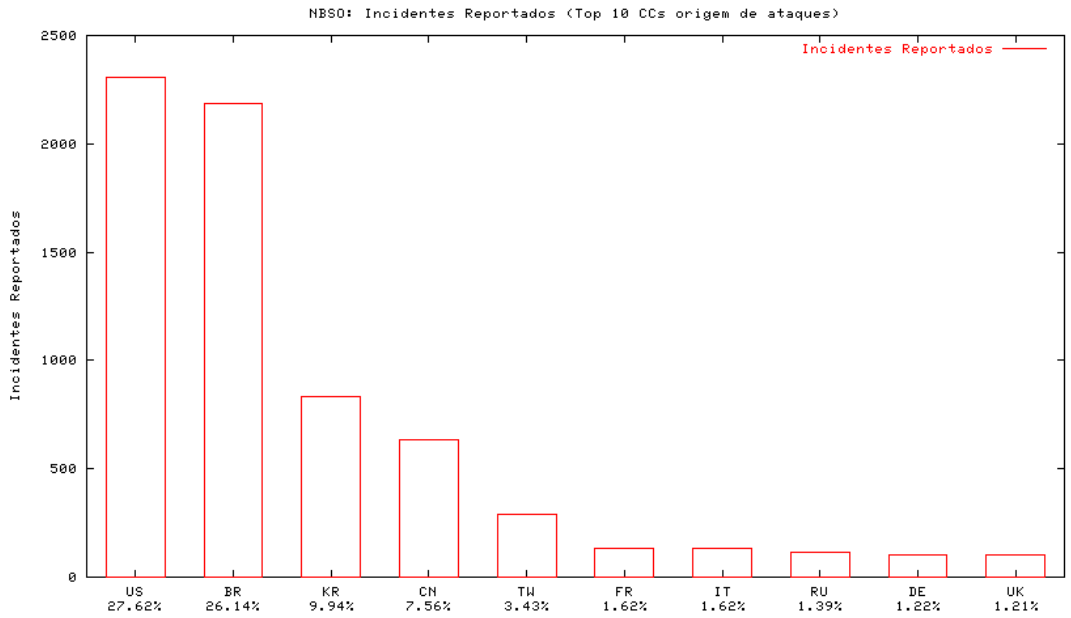


FIGURA 2: Dados sobre incidentes reportados ao Centro de Atendimento a Incidentes de Segurança - CAIS, mensalmente, nos últimos 6 anos (CAIS, 2005)

Apesar do Brasil não ser o país com o maior número usuários de Internet do mundo, é ainda assim um dos países da onde se origina a maioria dos crimes cometidos por meio da Internet, ficando atrás apenas dos Estados Unidos.

O número de incidentes (26,14%) reportados no primeiro trimestre de 2005 no Brasil é muito próximo do número de incidentes (27,62%) reportados nos Estados Unidos no mesmo período (figura 3).

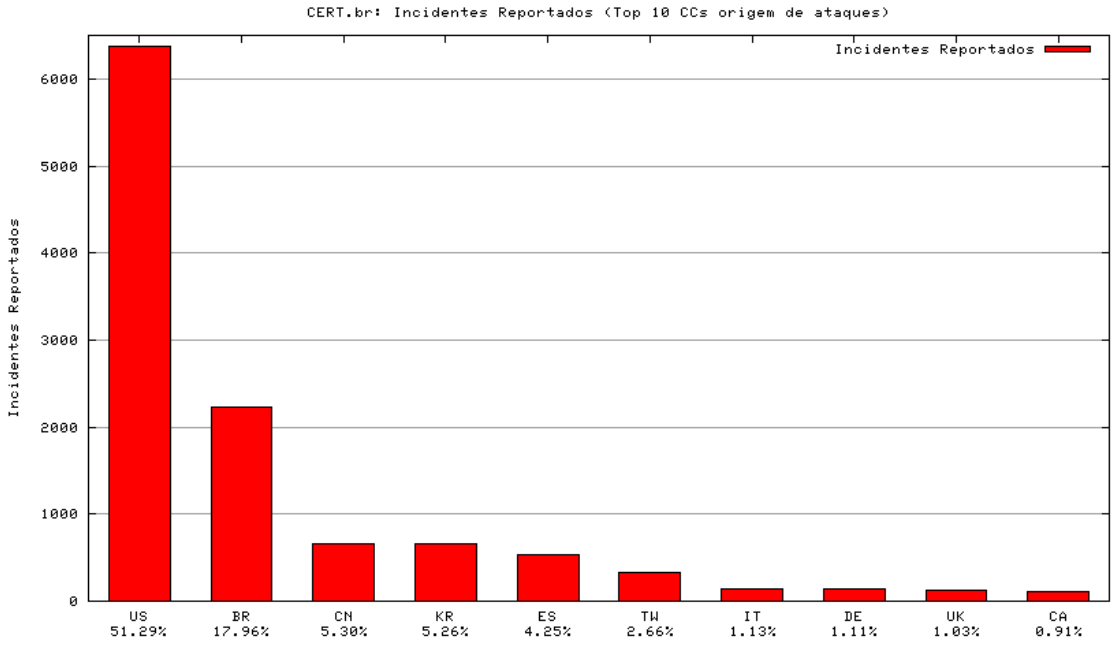


Observação: Este gráfico não inclui os dados referentes a worms.

FIGURA 3: Dados sobre a % de incidentes reportados ao CERT classificados por país no período de janeiro a março de 2005 (CERT, 2005)

No período compreendido entre abril e junho de 2005 o número de incidentes (17,96%) na Internet reportados no Brasil diminui em relação ao primeiro trimestre (figura 4). No entanto, o Brasil permanece como o segundo país com maior número de registros de incidentes na Internet.

Estes dados parecem confirmar as informações oriundas da Polícia Federal que afirma que 8 de cada 10 hackers vivem no Brasil (AGÊNCIA BRASIL, 2004).



Observação: Este gráfico não inclui os dados referentes a worms.

FIGURA 4: Dados sobre a % de incidentes reportados ao CERT classificados por país no período compreendido entre abril e junho de 2005 (CERT, 2005)

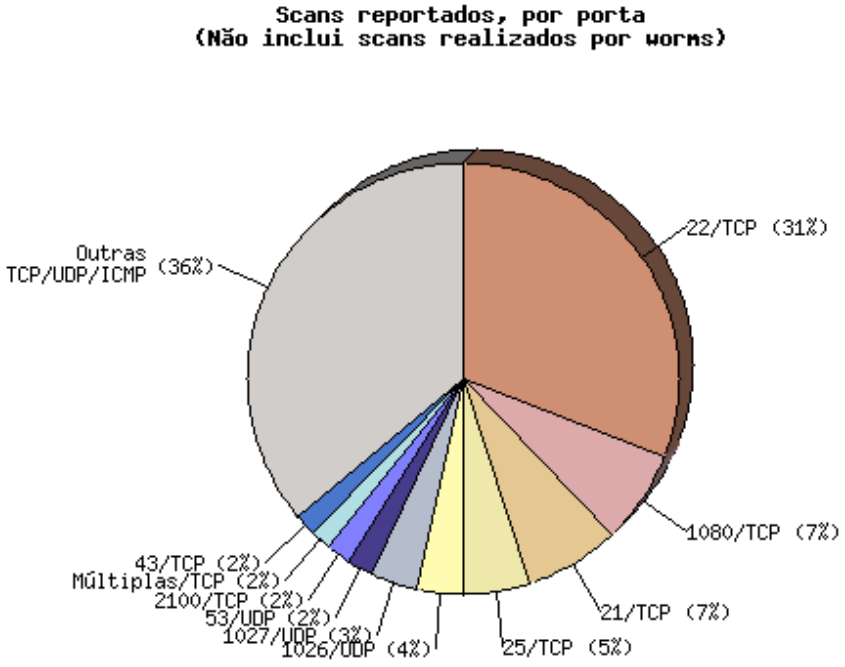
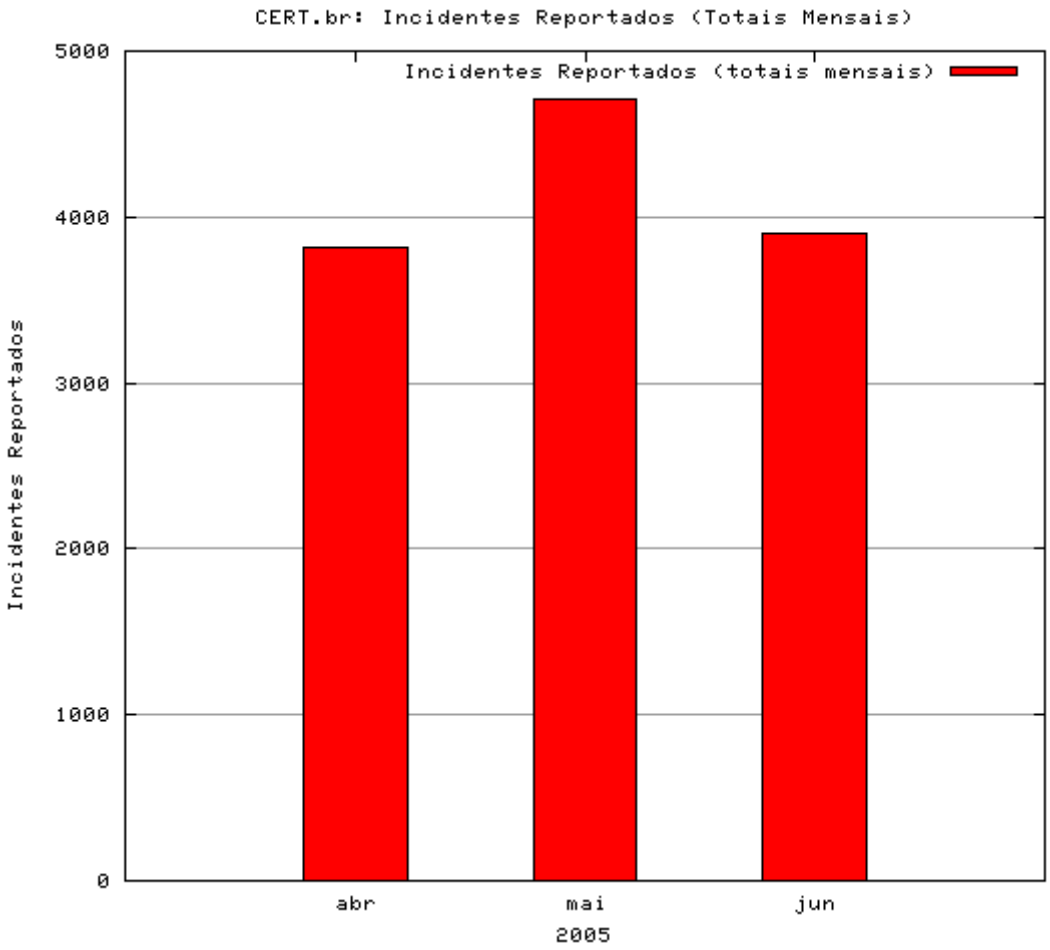
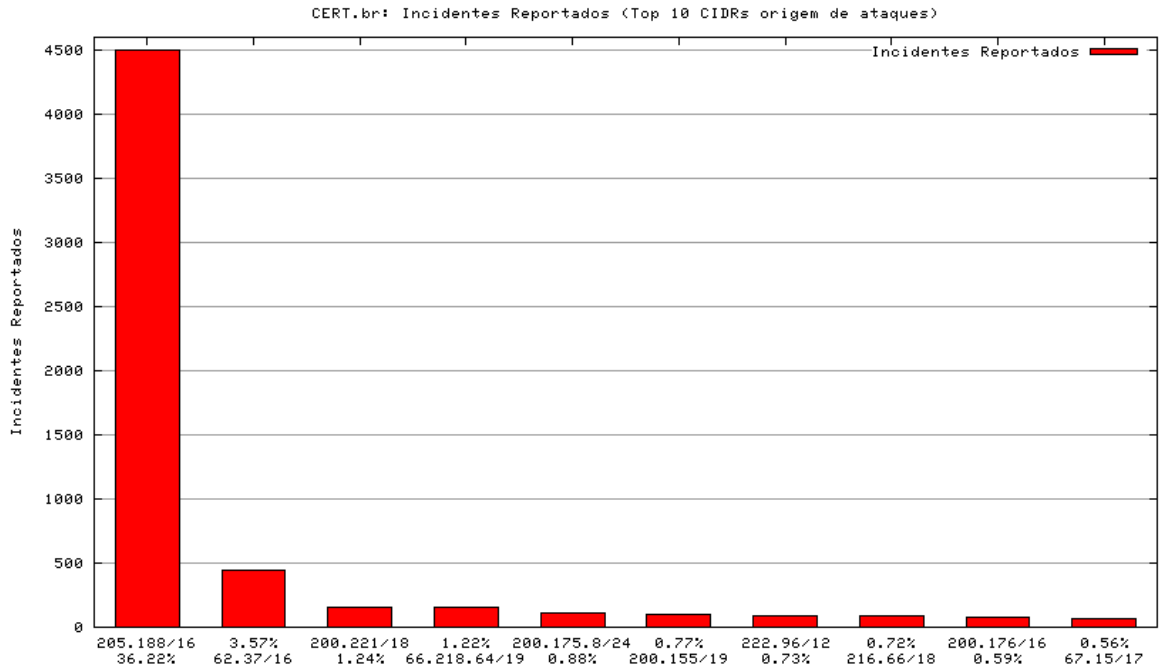


FIGURA 5: Dados referentes ao scans reportados por porta ao CERT de Abril a Junho de 2005 (CERT, 2005)



Observação: Este gráfico não inclui os dados referentes a worms.

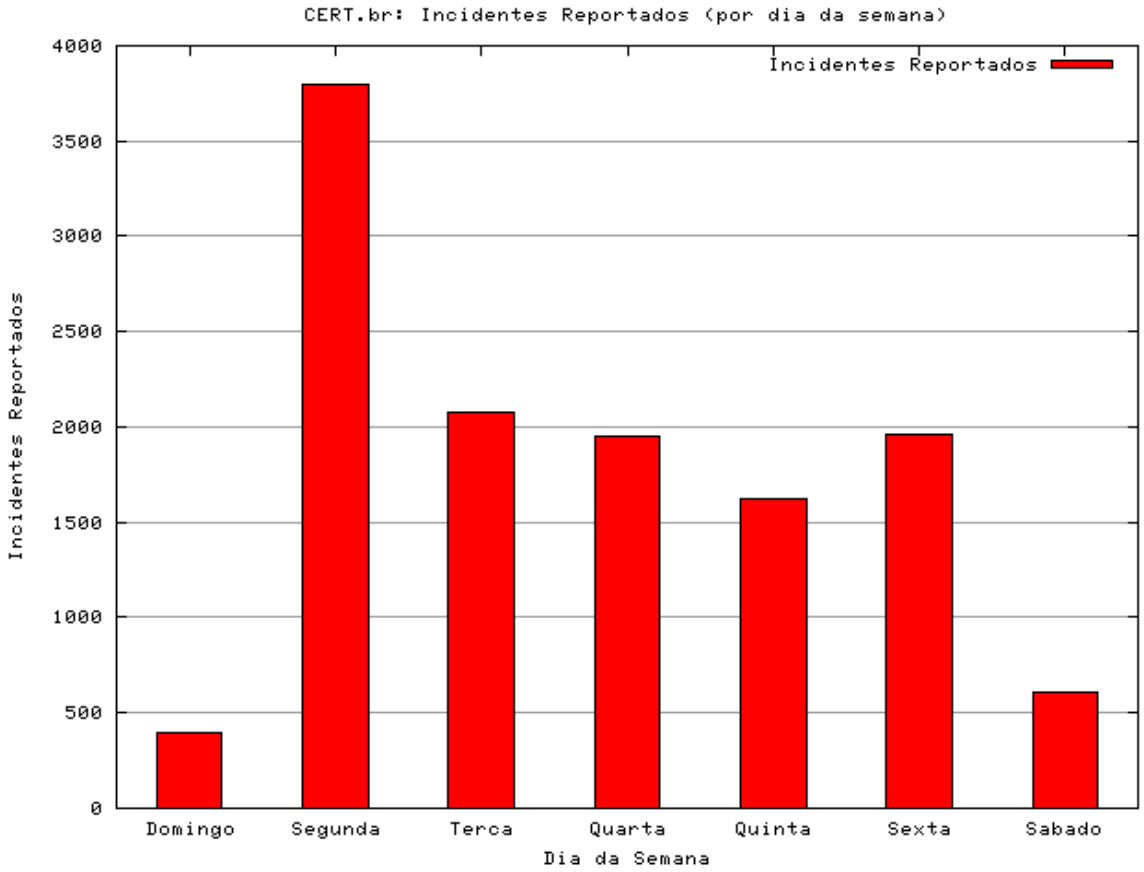
FIGURA 6: Dados referentes ao número de ataque reportados ao CERT no período de abril a junho de 2005 (CERT, 2005)



Observação: Este gráfico não inclui os dados referentes a worms.

FIGURA 7: Dados referentes aos ataques reportados ao CERT por origem de ataque no período entre Abril a Junho de 2005 (CERT, 2005)

Os dados da figura 8 mostraram que a segunda-feira foi o dia da semana que ocorreu um maior número de registro de ataques reportados ao CERT (2005). Este dado pode indicar que os ataques ocorrem mais freqüentemente no final de semana. Talvez nestes dias os hackers tenham um tempo maior para se dedicarem às atividades criminosas e também que devido ao fato de muitos usuários acessarem a Internet apenas em seu local de serviço o delito só é observado na segunda-feira, dando tempo ao hacker de fazer muitas vitimas sem ser descoberto.



Observação: Este gráfico não inclui os dados referentes a worms.

FIGURA 8: Dados referentes ao número de ataque reportados ao CERT por dia da semana, no período entre abril e junho de 2005 (CERT, 2005)

Os dados da tabela 2 indicaram que os tipos de ataques que com maior número de registro no CERT ocorridos no Brasil no período compreendido entre abril e junho de 2005 foram: as fraudes; os worm e os scans.

TABELA 2: Informações referente aos tipos de ataques ocorridos no período entre abril a junho de 2005. (CERT, 2005)

.

Mês	Total	worm (%)		af (%)		dos (%)		invasão (%)		aw (%)		scan (%)		fraude (%)	
Abr	**5253**	1432	27	17	0	0	0	20	0	25	0	1437	27	2322	44
Mai	**6883**	2175	31	4	0	2	0	34	0	22	0	1489	21	3157	45
Jun	**5406**	1510	27	0	0	5	0	17	0	55	1	1356	25	2463	45
Total	**17542**	5117	29	21	0	7	0	71	0	102	0	4282	24	7942	45

Legenda: af: Ataque ao usuário final; dos: Denial of Service; aw: Ataque a servidor Web

Os registros do CERT (2005) mostraram que 45% dos cibercrimes reportados no Brasil entre abril e junho de 2005 eram fraudes; 29% eram worm, 24% scan e 1% ataques ao servidor web (figura 9).

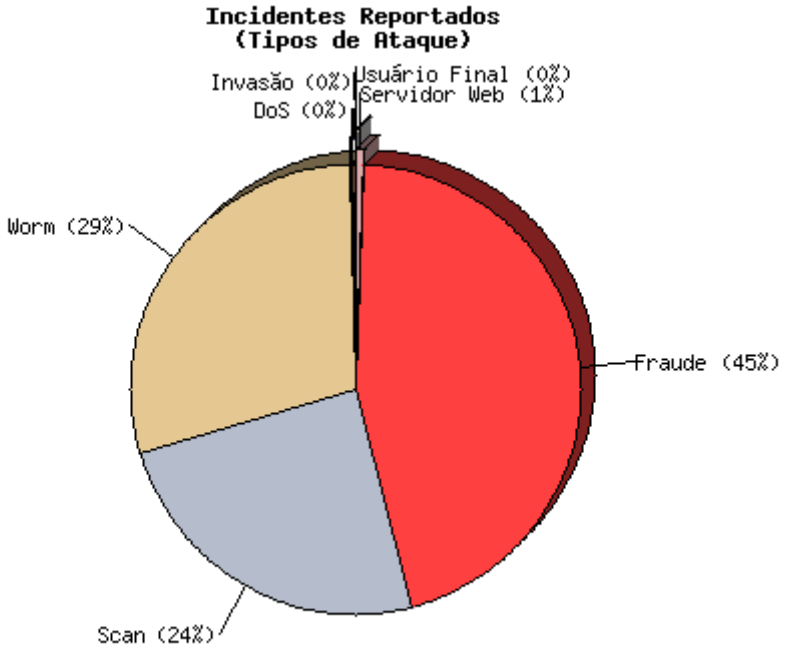


FIGURA 9: Dados referentes ao tipo de ataque reportados ao CERT no período entre abril a Junho de 2005 (CERT, 2005)

A fraude na Internet é bastante facilitada, pois o criminoso se aproveita da ingenuidade dos usuários e da facilidade em se manter anônimo ou assumir uma identidade que não a sua no meio eletrônico.

Estes fatores contribuem para que estes criminosos muitas vezes permaneçam impunes ou até mesmo acusem injustamente pessoas inocentes.

Em 2005 a Polícia Federal realizou diversas operações com o objetivo de combater fraudes pela Internet.

A Operação Clone foi desencadeada no dia 16 de fevereiro em Brasília (DF) com o objetivo de prender uma quadrilha que lesava centenas de correntistas por meio de fraudes bancárias. Quatro pessoas foram presas. De acordo com as investigações, o grupo executava fraudes através da Internet e obtinha, por meio de empregados dos bancos, os saldos e dados pessoais dos clientes a serem lesados. O principal alvo da quadrilha era a Caixa Econômica Federal, mas foram registradas ocorrências contra correntistas do Banco do Brasil, Itaú e Bradesco no Distrito Federal e nos estados do Rio de Janeiro, Goiânia, Ceará e São Paulo. Os valores desviados chegaram a 10 milhões de reais, conforme informações da Agência de Notícias da Polícia Federal (2005).

O segundo tipo de crime mais registrado no Brasil e que provoca um grande dano ao usuário é o worm, que constitui em códigos de programas maléficos inseridos no computador do usuário que tem por finalidade roubar informações, prejudicar a integridade do sistema ou até mesmo fazer com que a máquina seja usada para fins ilícitos que o atacante tenha vontade.

De acordo com a CARTILHA DE SEGURANÇA PARA INTERNET (2005):

> *Worm* é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores. Geralmente o *worm* não tem como conseqüência os mesmos danos gerados por um vírus, como por exemplo a infecção de programas e arquivos ou a destruição de informações. Isto não que dizer que não represente uma ameaça à segurança de um computador, ou que não cause qualquer tipo de dano. *Worms* são notadamente responsáveis por consumir muitos recursos. Degradam sensivelmente o desempenho de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar. Além disso, podem gerar grandes transtornos para aqueles que estão recebendo tais cópias.

Para a RFC (Request for Comment) 1135 (TURBAN e KING, 2004) “Um worm é um programa que pode rodar independentemente, consumindo recursos de seu hospedeiro por dentro para poder manter-se e propagando uma versão funcional completa de si para outra máquina.”

A disseminação de worm poder ser feita por meio de e-mails, arquivos infectados e pelo acesso a sites de pessoas má intencionadas. Ele se espalha muito rapidamente pelos computadores, geralmente, afeta um número grande de usuários, muito dos quais nunca chegam a ter conhecimento de que foram infectados. São parecidos com vírus, mas independem de outros programas e se alastram pela Internet e pelo computador de uma maneira mais veloz do que o vírus e por isso se tornam perigosos. Devido a sua velocidade e ao grande volume de replicação eles acabam gerando um tráfego muito grande na rede o que provoca demora em serviços de web, tais como abrir uma página.

Outro tipo de programa malicioso que Turban e King (2004) citam com alguma importância é o Cavalo de Tróia, que consiste num programa que depois de instalado na máquina alvo, ela fica a total disposição do hacker para ele fazer o que quiser, tendo ele acesso total aos recursos da máquina. E esses programas sempre vêm ocultos dentro de programas com alguma utilidade, por isso se tornam tão perigosos. Normalmente eles vêm escondidos dentro de jogos simples feito em flash e algumas animações, como também podem vir dentro de vários outros programas, até mesmo programas conhecidos que tenham sido modificados pelo hacker para conter o cavalo de tróia.

Incidentes devido ao scam aparecem em terceiro lugar no registro do CERT (2005).

Scam é o roubo de informação de uma pessoa, tais como informações de contas bancárias, de cartões de crédito. O scam muitas vezes é o inicio de uma fraude. O criminoso rouba informações de diversos usuários a partir de um scan ou phishing scan.

Segundo a Folha de São Paulo (2005) um dos golpes mais comuns utilizados por criminosos virtuais é enviar uma mensagem alertando sobre possíveis invasões de contas, registro como inadimplentes na Serasa ou irregularidades na Receita Federal (figura 10, 11, 12). Nessas mensagens são pedidos para que os usuários digitem seus dados: banco, agência, conta e senha. Outra forma comum de ação é a criação das chamadas páginas clone das instituições bancárias, para onde os usuários são direcionados quando tentam acessar a página do seu banco. Todos esses métodos tentam "pescar" a senha dos usuários, o que vem sendo chamado pela comunidade virtual de "phishing", expressão resultante das palavras "password" (senha) e "fishing" (pesca). Até o momento, não foi identificado nenhum ataque direto aos sistemas bancários.

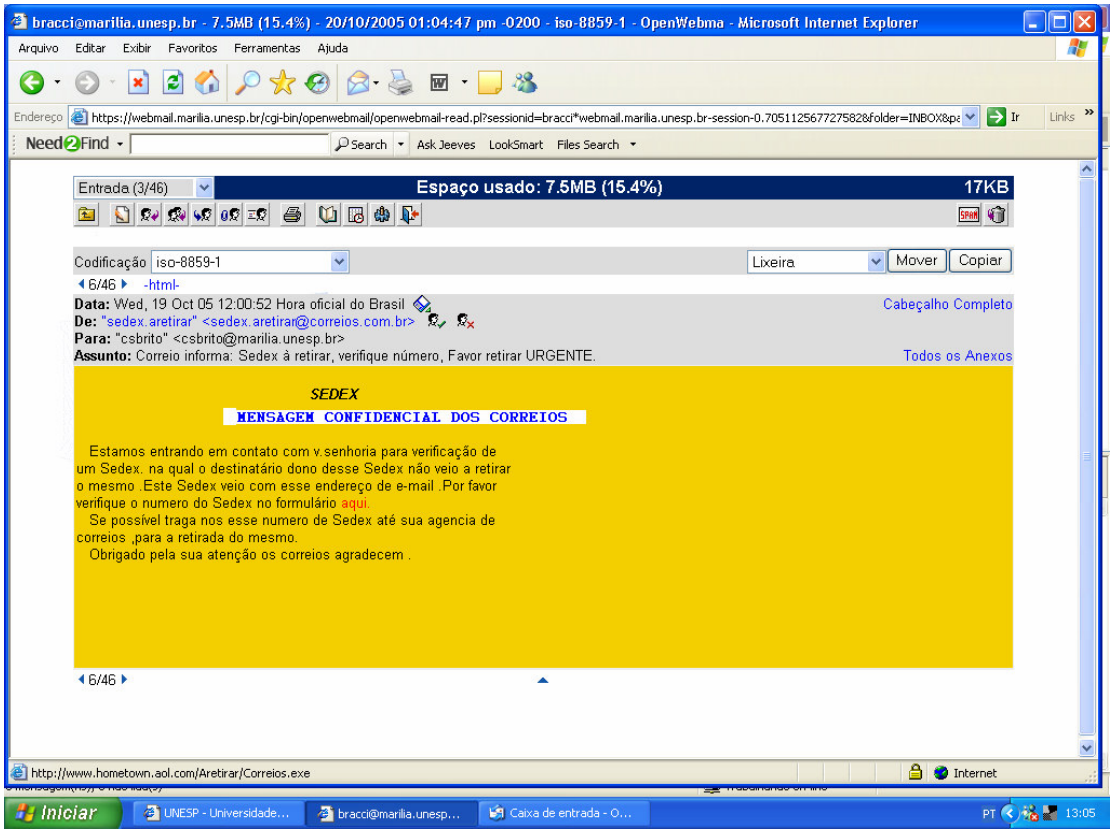


FIGURA 10 – Exemplo de fishing

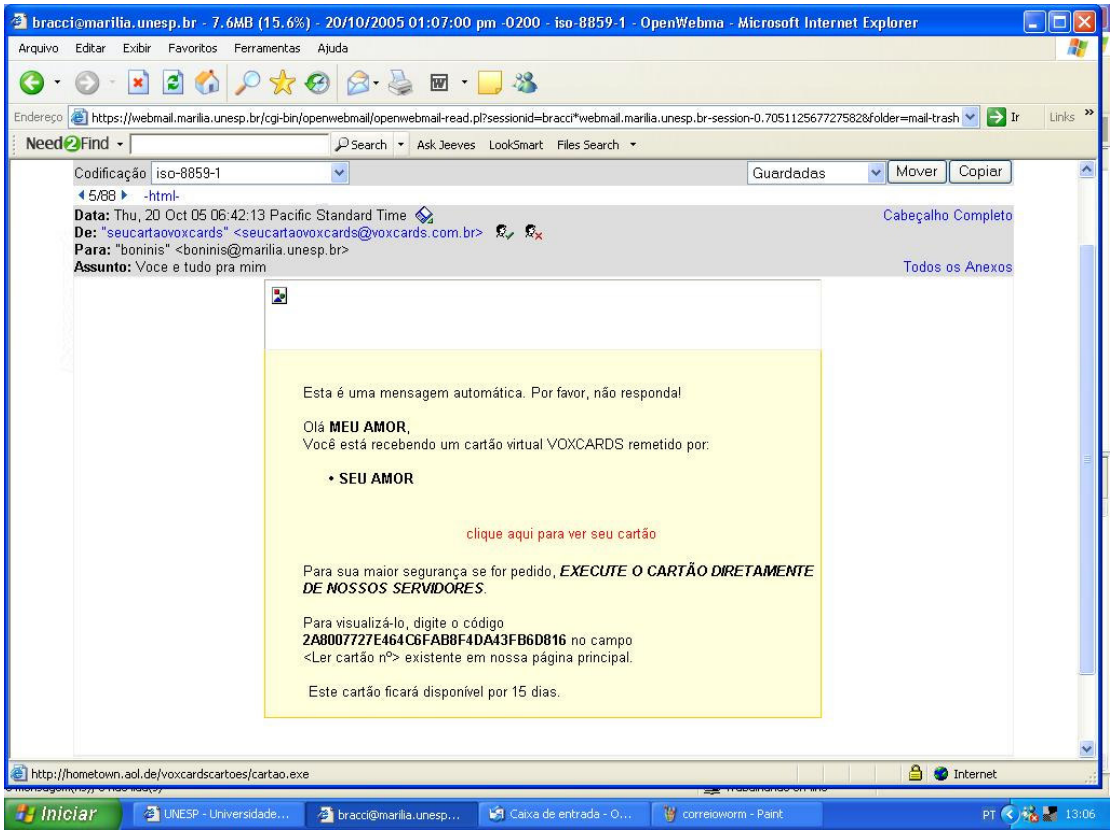


FIGURA 11 – Exemplo de fishing

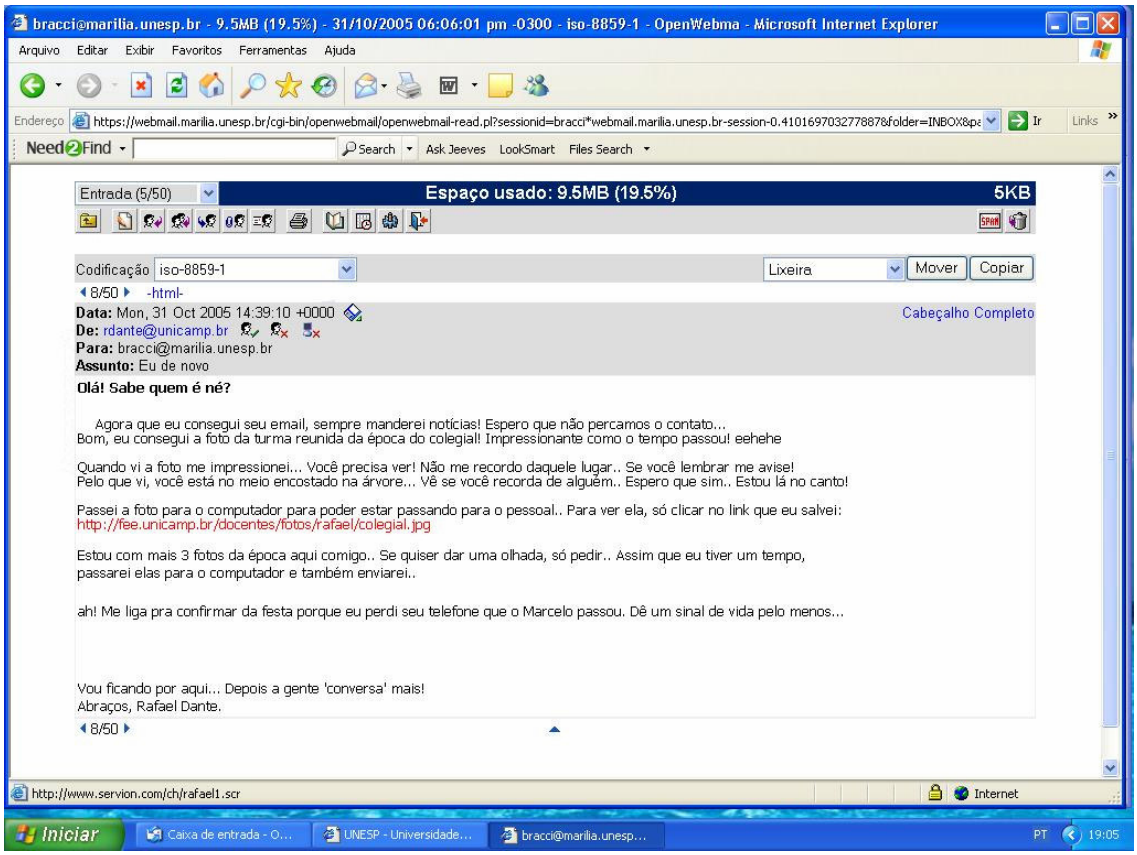


FIGURA 12 – Exemplo de fishing

No dia 11 de agosto, a Polícia Federal, desencadeou a Operação Encaixe para desarticular uma quadrilha especializada na clonagem de cartões de bancos, que eram usados para movimentações entre contas e saques em caixas eletrônicos, principalmente da Caixa Econômica Federal. O grupo atuava desde 2003, em Belo Horizonte, no interior de Minas Gerais e no Espírito Santo.

O ataque a servidores web, ou cibervandalismo, contribui com 1% dos crimes reportados no Brasil. Este tipo de ataque consiste em invadir, alterar e prejudicar um site por meio de invasão de seu servidor.

Outro tipo de ataque citado por Turban e King (2004) é o ataque distribuído de recusa de serviço, ou DdoS (distributed denial of service). O ataque de recusa de serviço (DoS - Denial of Service) é um ataque onde o atacante se utiliza de algum programa especialista em enviar milhares de pacotes a um computador alvo a fim de sobrecarregar os recursos da máquina vítima. Já no ataque distribuído de recusa de serviço, ou DdoS, Turban e King (2004) descreveram seu funcionamento da seguinte maneira:

> No ataque distribuído de negação de serviço o atacante obtém acesso administrativo ilegal ao maior número possível de computadores na internet. Uma vez obtido o acesso a um grande número de computadores, o hacker carrega neles um software DdoS especializado. O software fica dormente, esperando receber um comando para iniciar o ataque. Quando o comando é dado, essa rede distribuída de computadores começa a enviar requisições ao computador-alvo.

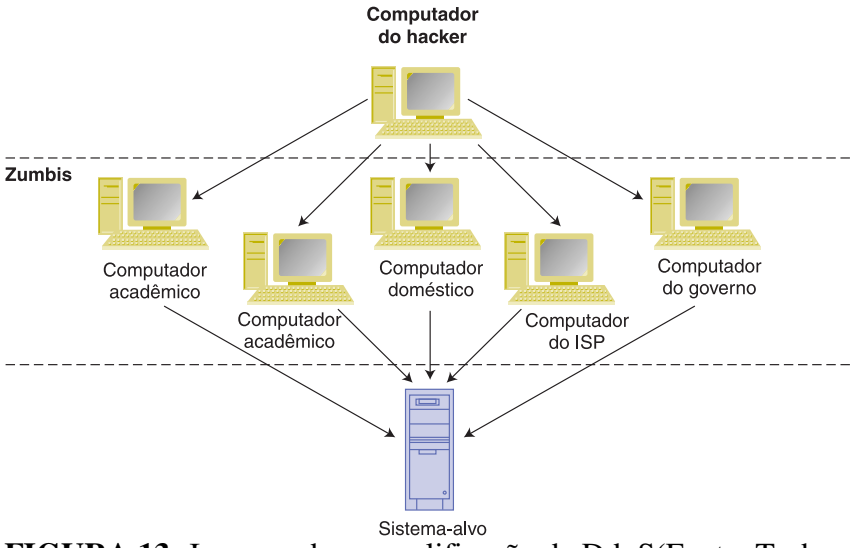


FIGURA 13: Imagem de exemplificação de DdoS(Fonte: Turban e King,2004)

A Polícia Federal realizou uma grande Operação, a Pégasus, que foi desencadeada no dia 25 de agosto, com objetivo de prender integrantes de uma organização criminosa especializada em invadir contas bancárias por meio da Internet. A ação ocorreu nos estados de Goiás, Pará, Distrito Federal, Tocantins, Maranhão, Espírito Santo, Minas Gerais e São Paulo. Os fraudadores, conhecidos popularmente como ‘hackers’ ou ‘crackers’, causavam prejuízos a correntistas de todas as grandes instituições bancárias no país desde 2001, e alguns deles já tinham sido presos em outras operações realizadas pela Polícia Federal. Esta operação foi um desdobramento das operações Cash Net (2001), Cavalo de Troia 1 (2003) e Cavalo de Tróia 2 (2004). Segundo as investigações, a subtração de valores das contas acontecia de três formas: transferência de valores depois sacados das contas alugadas, aquisição de produtos e serviços comercializados pela internet ou pagamento de boletos diversos (impostos, taxas, produtos ou serviços). Em todos os casos, os débitos aconteciam sempre em contas das vítimas que tiveram suas senhas capturadas pela internet através do programa conhecido como "cavalo de tróia" ou "trojan". Já há indícios do uso desses programas, criados pela quadrilha no Brasil, em países como Estados Unidos e Venezuela. Os estelionatários descobriam os dados bancários invadindo o computador da vítima por meio do programa "trojan", que geralmente é

enviado via e-mail para o usuário desinformado que rodava o programa e assim infectava seu computador com o “trojan” e assim permitindo aos hackers terem acesso a suas informações. O programa se encarregava de mandar as informações para um servidor, ou caixa de e-mail dos criminosos. Essa foi a primeira grande operação coordenada pela recém-criada DRCC (Divisão de Repressão a Crimes Cibernéticos) da Polícia Federal. Os acusados responderam pelos crimes de furto qualificado (artigo 155 do Código Penal), formação de quadrilha (artigo 288 do mesmo código) e violação do sigilo bancário (artigo 10 da Lei Complementar 105/2001). As penas podem chegar a oito anos de prisão. (FOLHA DE SÂO PAULO ON-LINE - dinheiro, 25/08/2005).

A pornografia infantil, apesar de não ter sido citada nos dados da CERT (2005), também, é um tipo de crime bastante praticado no Brasil.

Este tipo de crime decorre da imensa facilidade para se compartilhar arquivos e informações pela Internet em completo anonimato. Esta facilidade no compartilhamento de informações estimula a distribuição desse tipo grotesco de arquivo.

Dados da Polícia Federal mostraram que no período entre 2001 e 2004 a denuncia de pedofilia no Brasil praticamente dobrou. No ano de 2001 a Polícia Federal registrou 2322 denúncias de pedofilia em 2005 ocorreram 5475 denúncias (figura 14).

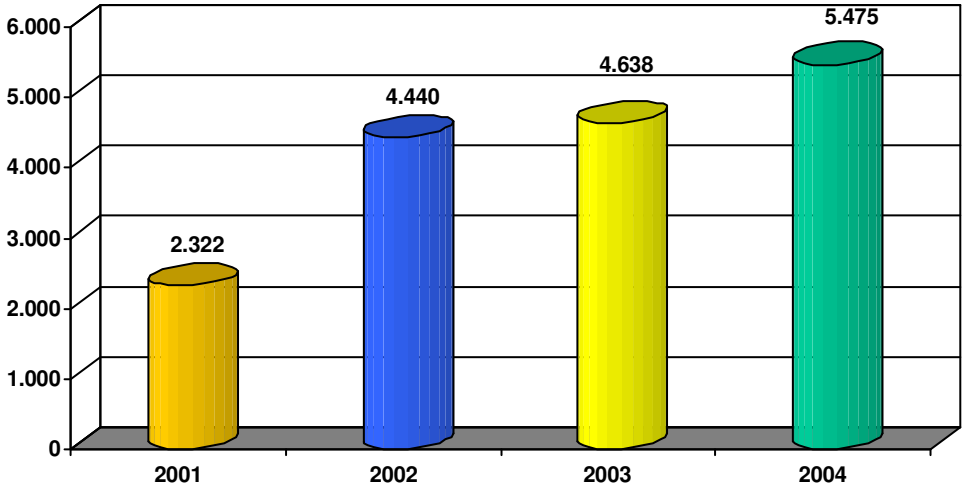


FIGURA 14: Dados sobre denúncia de pedofilia na web no Brasil (Fonte: relatório 2004 Polícia Federal)

Exemplo do desdobramento deste tipo de crime foi a Operação Anjo da Guarda, da Polícia Federal, que consistiu em ações para prender pessoas envolvidas com pedofilia. No dia 7 de junho, cumpriu 18 mandados de busca e apreensão em oito estados, com o objetivo de recolher material de informática, fitas e CD's contendo pornografia infantil. Foi preso o professor de lutas marciais A. L. J. B. C., de 33 anos, por ter produzido, divulgado e trocado no exterior, via internet, fotos e vídeos de atos sexuais com menores de idade. A segunda fase da Operação Anjo da Guarda, denominada Anjo da Guarda II, prendeu no dia 31 de agosto, cinco pessoas acusadas de produzir e divulgar através da Internet fotos e vídeos contendo pornografia infantil. Os policiais chegaram aos acusados graças às apreensões realizadas no dia 07 de junho deste ano, na primeira fase da operação.

No ano de 2005 a policia federal realizou diversas operações destinadas à prisão de pessoas envolvidas com cibercrimes (tabela 2). As operações de maior sucesso foram: clone, anjo da guarda; encaixe; pegasus; anjo da guarda II (Polícia Federal, 2005).

TABELA 3: Operações desenvolvidas pela polícia federal (FONTE: Polícia Federal, 2005)

Presos em 2005				
Operação	**Total**	**Servidores Públicos**	**Policiais Federais**	**Data**
Alcatéia	**11**	**0**	**0**	**jan/05**
Predador	**15**	**0**	**0**	**jan/05**
Petisco	**43**	**4**	**0**	**fev/05**
Pretorium	**7**	**5**	**0**	**fev/05**
Big Brother	**5**	**0**	**0**	**fev/05**
Clone	**4**	**0**	**0**	**fev/05**
Terra Nostra	**15**	**3**	**0**	**fev/05**
Caronte	**22**	**14**	**0**	**fev/05**
Ajuste Fiscal	**11**	**11**	**0**	**fev/05**

Dragão	**5**	**0**	**0**	**mar/05**
Buritis	**29**	**14**	**0**	**mar/05**
Março Branco	**8**	**5**	**0**	**abr/05**
Tango	**13**	**0**	**0**	**abr/05**
Castanhola	**12**	**0**	**0**	**abr/05**
Hidra	**67**	**21**	**1**	**maio/05**
Guabiru	**26**	**10**	**0**	**maio/05**
Curupira	**101**	**50**	**0**	**jun/05**
Anjo da Guarda	**1**	**0**	**0**	**jun/05**
Panorama	**26**	**0**	**0**	**jun/05**
Cevada	**72**	**0**	**0**	**jun/05**
Tentáculos	**28**	**9**	**0**	**jun/05**
Tâmara	**19**	**0**	**0**	**jun/05**
Mercúrio	**38**	**18**	**0**	**jun/05**
Monte Éden	**28**	**0**	**0**	**jun/05**
Narciso	**3**	**0**	**0**	**jul/05**
Confraria	**6**	**1**	**0**	**jul/05**
Lion Tech	**6**	**0**	**0**	**ago/05**
Falsário	**4**	**2**	**0**	**ago/05**
Macunaíma	**0**	**0**	**0**	**ago/05**
Babilônia	**7**	**0**	**0**	**ago/05**
Matinta Perêra	**24**	**7**	**0**	**ago/05**
Encaixe	**7**	**0**	**0**	**ago/05**
Caá-Ete	**31**	**3**	**0**	**ago/05**
Curupira	**16**	**2**	**0**	**ago/05**
Serraluz	**34**	**4**	**0**	**ago/05**
Pégasus	**114**	**0**	**0**	**ago/05**
Roupa Suja	**11**	**0**	**0**	**ago/05**
Trevo	**20**	**1**	**0**	**ago/05**
Anjo da Guarda	**5**	**0**	**0**	**ago/05**
Mercado Negro	**26**	**9**	**0**	**set/05**
Total	**744**	**183**	**1**	

Em relação aos cibercrimes que afetam diretamente as pessoas jurídicas dados obtidos na 9ª Pesquisa Nacional de Segurança da Informação (Módulo Security, 2003) concluíram que as cinco principais ameaças à segurança das informações nas empresas foram: vírus (66%), funcionários insatisfeitos (53%), divulgação de senhas (51%), acessos indevidos

(49%) e vazamento de informações (47%) (figura 15). Os dados desta pesquisa mostraram, também, que 35% das empresas entrevistadas admitiram que tiveram perdas financeiras em 2003. Desse total, 22% registraram perdas de até R$ 50 mil, 8% entre R$ 50 mil a R$ 500 mil e 4% de R$ 500 mil a R$ 1 milhão.

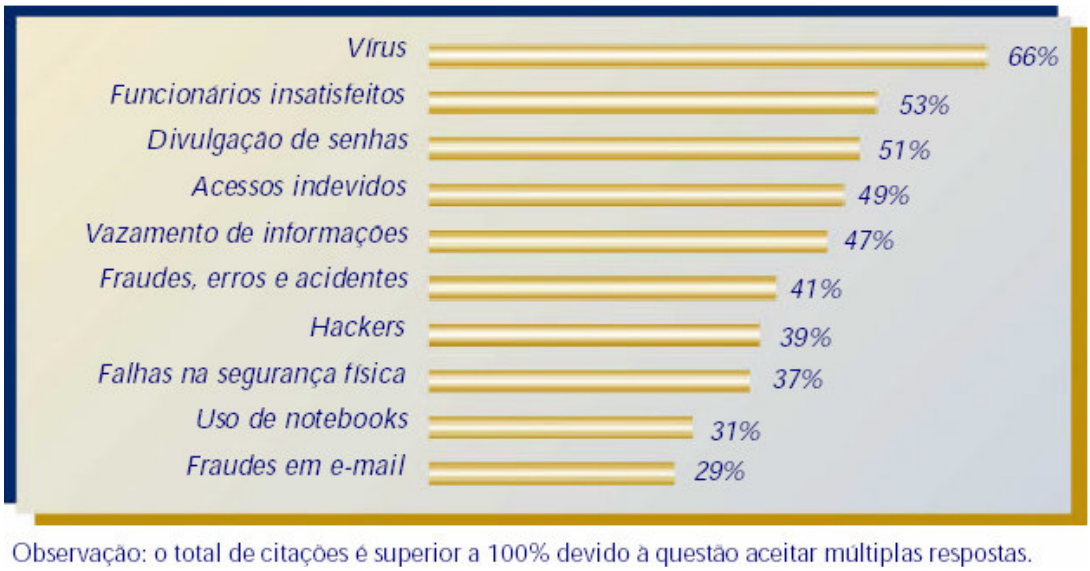


FIGURA 15: Dados referentes aos principais tipos de fraudes na internet (FONTE: Módulo Security, 2003).

Observa-se que todos estes fatores estão direta ou indiretamente relacionados à ação humana.

Muitas vezes funcionários com acesso autorizado, porém desatentos e com pouco treinamento, podem tornar-se causa potencial de incidentes segurança (MOREIRA, 2001).

Para Ferreira (2005) a grande maioria dos incidentes em relação à segurança tem a intervenção humana, seja de forma acidental ou não. Segurança tem a ver com pessoas e processos, antes de ter a ver com tecnologia. Conseqüentemente, de nada valerão os milhões investidos em Tecnologia da Informação (TI) se o fator humano for deixado em segundo plano. Quanto melhor preparados os funcionários de uma organização, mais segura ela será.

2 Questões legais de crimes virtuais

Na doutrina brasileira, tem-se apregoado que os cibercrimes podem ser puros (próprios) e impuros (impróprios). São considerados puros ou próprios, aqueles crimes que foram praticados por computador e se realizaram ou se consumiram em um meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado. Os cibercrimes impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultados naturalísticos, que ofenda o mundo físico ou o espaço real, ameaçando ou lesando outros bens, não-computacionais ou diversos da informática (RODRIGUES, 2004).

No Brasil os legisladores começam a se preocupar apenas recentemente com as questões referentes à regulamentação e a penalização dos crimes cometidos virtualmente ou com o auxílio da informática.

Entre as leis vigentes no Brasil algumas, como o Estatuto da Criança e do Adolescente, a Constituição Federal e o Código Penal, já passaram por modificações para se adequarem à realidade atual e combaterem o crime virtual.

A lei nº 8.069, de 13 de julho de 1990, que dispõe sobre o estatuto da criança e do adolescente afirma em sua seção II que é crime:

> Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente (Redação dada pela Lei nº 10.764, de 12.11.2003)

A lei nº 9.296, de 24 de julho de 1996, que regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal afirma que:

> Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.

> Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

O decreto-lei nº 2.848/40, de 7 de dezembro de 1940, Código Penal, em seu TÍTULO XI, CAPÍTULO I - dos crimes praticados por funcionário público contra a administração em geral, considera crime e prevê pena de reclusão em seus artigos 313-A; 313-B; 325

> **Inserção de dados falsos em sistema de informações** (Incluído pela Lei nº 9.983, de 2000)
> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (Incluído pela Lei nº 9.983, de 2000)
> Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa. (Incluído pela Lei nº 9.983, de 2000)
>
> **Modificação ou alteração não autorizada de sistema de informações** (Incluído pela Lei nº 9.983, de 2000)
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: (Incluído pela Lei nº 9.983, de 2000)
> Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa. (Incluído pela Lei nº 9.983, de 2000)
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.(Incluído pela Lei nº 9.983, de 2000)
>
> **Violação de sigilo funcional**
> Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação:
> Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.
> § 1º Nas mesmas penas deste artigo incorre quem: (Incluído pela Lei nº 9.983, de 2000)
> I - permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública; (Incluído pela Lei nº 9.983, de 2000)
> II - se utiliza, indevidamente, do acesso restrito. (Incluído pela Lei nº 9.983, de 2000)
> § 2º Se da ação ou omissão resulta dano à Administração Pública ou a outrem: (Incluído pela Lei nº 9.983, de 2000)
> Pena - reclusão, de 2 (dois) a 6 (seis) anos, e multa. (Incluído pela Lei nº 9.983, de 2000)

O Decreto nº 3.505, de 13 de junho de 2000, instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. No parágrafo 2º do

segundo artigo foram definidos os conceitos e os objetivos para a política de segurança do Governo Federal.

> Art. 2º Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações:
> II - Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

Para Gomes (2001) a publicação do Decreto nº 3.505 o Governo Federal definiu os pilares da segurança da informação, que são: a confidencialidade, a integridade e a disponibilidade das informações, em qualquer tipo de suporte, elegendo como integrantes do sistema de segurança não somente os programas, mas os recursos humanos e as instalações físicas.

Atualmente tramitam, no poder legislativo em Brasília, dois projetos de Lei com o objetivo de tipificar e penalizar os crimes informáticos no Brasil.

O Projeto de Lei nº 84/99 (2005), atualmente 89/03, de autoria do deputado Luiz Piauhylino, já foi aprovado pela Câmara dos Deputados e esta em trâmite no Senado Federal. Este projeto dispõe sobre os crimes cibernéticos e impõe penalidades para uma série de condutas ilícitas específicas cometidas no ambiente virtual.

O Projeto de Lei nº 4.144/04 (2005), de autoria do deputado federal Marcos Abramo, complementa o Projeto de lei citado anteriormente e visa adequar as leis brasileiras vigentes e futuras ao que estabelece a Convenção Européia sobre Cibercrimes.

Em 23 de Novembro de 2001, em Budapeste, na Hungria, os Estados Unidos e outros 29 países assinaram Tratado Internacional para Combater o Cibercrime. Este foi o primeiro instrumento elaborado para combater os problemas relacionados a propagação da atividade criminal em redes de computador.

Esta convenção solicitou esforços dos países participantes para estabelecerem leis que combatam ao cibercrime, asseguram ao judiciário a autoridade processual necessária para investigar eficazmente e punir as ofensas do cibercrime e forneçam a cooperação internacional a outros países na luta contra o crime relacionado ao computador (Cybercrime Convention, 2001).

2.1 Questões éticas

Ética não é nada além do que a área da filosofia que estuda a concepção de certo e errado. A ética define os padrões que serão considerados normais e corretos para uma determinada sociedade ou cultura. Ética é citada por Arruda (2004) como sinônimo de moral, ou o que deve ser considerado normal numa sociedade.

A análise etimológica da palavra mostra que ética vem do grego "ethos", e significa "hábito". Moral vem do latim "mores" e significa "hábito, costumes". Assim, não existiria o porque diferenciar filosoficamente ética de moral.

No entanto Imaguire (2000) afirmou:

> Fato é que mesmo no mundo filosófico existe um certo caos terminológico neste respeito. Especialmente na tradição teológica: o que os protestantes chamam de ética, os católicos chamam de moral. Em geral, procura-se seguir a seguinte distinção: enquanto a moral é uma ciência descritiva (descreve como os seres humanos de uma determinada cultura de fato agem) a ética é normativa (ele determina como eles deveriam agir). Dando um exemplo: sair nu pela Avenida Paulista seria imoral (em geral não se faz isso), mas não anti-ético (afinal, não se está fazendo mal a ninguém!). Mas observe: nem todos os filósofos fazem tal distinção: o grande Kant, por exemplo, tende a usar "moral" no sentido que aqui explico como "ética"! Portanto: sempre observe de quem se está a falar.
> Além disso, as coisas não são tão fáceis como na distinção proposta: o que em geral não se faz numa sociedade pode ser prejudicial e assim talvez automaticamente antiético (a nudez na Avenida Paulista poderia estar pervertendo adolescentes, levando-os para um "mau caminho", por exemplo, e isto já seria antiético). Além disso chama-se ética, em geral, diferindo novamente da moral, a ciência que trata apenas do conhecimento natural (não aquele revelado por Deus na Bíblia) sobre o Bem e o Mal. Ou seja, um ateu deveria por si só, sem crer na Bíblia, saber o que é Bem e o que é Mal.

> A ética se basearia portanto apenas na capacidade individual e natural da razão.

Para se discutir ética é preciso primeiro estudar o conceito de metafísica, que Marchionni (1999, p. 36) descreve como:

> Definimos metafísica a maneira mais profunda, a mais profunda possível, de encarar as coisas, os entes. A metafísica sonda tudo aquilo que pode ser expiementado pelo homem, quer se trate de percepção sensível ou imaginação ou sentimento ou pensamento especulativo ou experiência poético-artística ou a experiência mística.

Para Kant (1997, p. 14):

> Pode-se chamar empírica a toda a filosofia que se baseie em princípios da experiência, aquela porem cujas doutrinas se apóiam em princípios a priori chama-se filosofia pura. Esta ultima, quando e simplesmente formal, chama-se Lógica; mas quando se limita a determinados objetos do entendimento chama metafísica.

Kant cita, ainda, que existem duas metafísicas, a metafísica da natureza e a metafísica do costume.

Todo este estudo da metafísica é necessário porque de acordo com estes autores a ética é algo que vai além das sensações físicas. Falar sobre a ética em relação à metafísica é falar sobre o bem ou mal absoluto, algo muito além de simples padrões morais.

De acordo com Marchionni (1999, p. 33):

> A ética é a arte que torna bom aquilo que é feito (operatum) e quem o faz (operantem). É a arte do bom. Ciência do bom... A ética torna bom aquilo que é feito. Ela é a idéia e pratica do bom, princípios e ações. O prisioneiro da caverna de Platão, que foi liberto da escuridão, após "muito esforço" chega a fixar o sol, a contemplar o bom, que o impulsiona a ações boas, a voltar a caverna para libertar os outros.

Sobre a ética, Aristóteles pregava a moderação para que se pudesse ter uma vida equilibrada e harmônica. Achava que a felicidade real era a integração de três fatores: prazer, ser cidadão livre e responsável e viver como pesquisador e filósofo. Cria também que devemos ser corajosos e generosos, sem aumentar ou diminuir a dosagem desses dois itens.

Aristóteles chamava o homem de ser político. Citava formas de governo consideradas boas como a monarquia, a aristocracia e a democracia. Acreditava que sem a sociedade ao nosso redor não éramos pessoas no verdadeiro sentido do termo.

Por este motivo falar sobre ética e, ainda, mais tentar buscar a relação entre ética e moral é sempre complicado.

Para Arruda (2004) a ética tem uma estreita relação com a moral e o direito. No entanto, apesar desta ligação, moral e direito são coisas diferentes.

Este tema é sempre conflituoso, pois nem sempre algo que é considerado eticamente errado poder ser, também, considerado legalmente errado. A diferença entre ética e moral pode ser exemplificada desta forma quando um amigo trai sua confiança todos dizem que isto é antiético, mas ainda assim não é algo ilegal.

Almeida (2004) Promotor de Justiça do MPDFT disse:

> O Direito, visto como ciência, é um conjunto de normas de cumprimento obrigatório, impostas pelo Estado aos cidadãos, e destinadas a regular as relações sociais. Diz-se, também, que uma pessoa tem um direito quando lhe é dada a possibilidade ou faculdade de agir de acordo com a norma.
> Alguns direitos do homem são tão importantes que são chamados de direitos fundamentais, aqueles que somente em hipóteses excepcionais podem ser desrespeitados pelo próprio Estado, tais como a vida, a liberdade, a igualdade entre as pessoas, a segurança e a propriedade. Para proteger estes direitos, devidamente relacionados na Constituição, são colocadas à disposição das pessoas as garantias fundamentais, que são instrumentos como o *habeas corpus* e o mandado de segurança.

2.1.1. Ética dos Hackers

Hackers antigamente não significava pessoa com más intenções, os crackers sim, aqueles que tem por objetivo quebrar, interromper ou violar algo, mas o nome de cracker no uso do senso comum ficou também com este sentido. Eram programadores experientes que utilizavam esta experiência para um bem maior, que era demonstrar falha em programas. Ao apontar estas falhas os programadores as corrigiam, o que possibilitava maior segurança para

os usuários de tal software. Nessa época os hackers tinham um código de ética que era respeitado, eles procuravam ajudar ao outros sem benefício próprio.

Hoje em dia este código mudou e a conotação de hacker começou a tomar uma imagem mais negativa. As pessoas que atualmente recebem tal "apelido" são vistas como má intencionadas.

Para Vasconcelos (2000) hackers são pessoas que tem conhecimentos reais de programação e de sistemas operacionais, principalmente, o Linux e o Unix, que são os mais usados em servidores da Internet. Conhece quase todas as falhas desegurança dos sistemas e está sempre em busca de outras. Desenvolve suas próprias técnicas e programas de invasão**.**

Por base nas definições já encontradas, de hackers e crackers, vamos aceitar ao menos para este trabalho os dois grupos, como grupos de pessoas com um grande conhecimento em informática que independente do motivo cometem atos ilícitos.

Além dos hackers existem outros grupos de vândalos digitais, tais como crackers e carders.

Cracker é considerado por Vasconcelos (2000) o "Hacker do Mal", que invade sistemas, rouba dados e arquivos, números de cartão de crédito, faz espionagem industrial e quase sempre provoca algum tipo de destruição, principalmente de dados.

As ações praticadas pelos crackers podem ser consideradas ilegais, mas não necessariamente antiética, uma vez que essas pessoas têm o seu próprio código de ética que difere inteiramente do código de ética da sociedade em geral.

2.1.2. Considerações sobre o uso da tecnologia

Muitos tipos de ataques feitos pela internet têm seu início dentro de sites que buscam proteger-se contra ataques, nesses sites há listas onde são expostos os principais problemas e falhas dos programas mais comumente usados a fim de que seus usuários fiquem atentos e se protejam contra algum tipo de ataque, mas como muitos não acessam, seus sistemas continuam vulneráveis. O fato de explorar este tipo de falha se da o nome de CVEs (Commom vulnerabilities and exposures) que significa Vulnerabilidades e exposições comuns.

Crime virtual do ponto de vista tecnológico é todo tipo de crime que é feito pelo uso da informática.

Um tipo freqüente de delito virtual é o phishing, anteriormente citado, que consiste em você literalmente pescar (“phish”) informações de usuários e utilizá-las para benefícios próprio. Outro fato muito observado é o fato de computadores de pessoas normais serem usados para fins ilícitos sem o conhecimento da pessoa, criando assim redes zumbis que são usadas por pessoas má intecionadas.

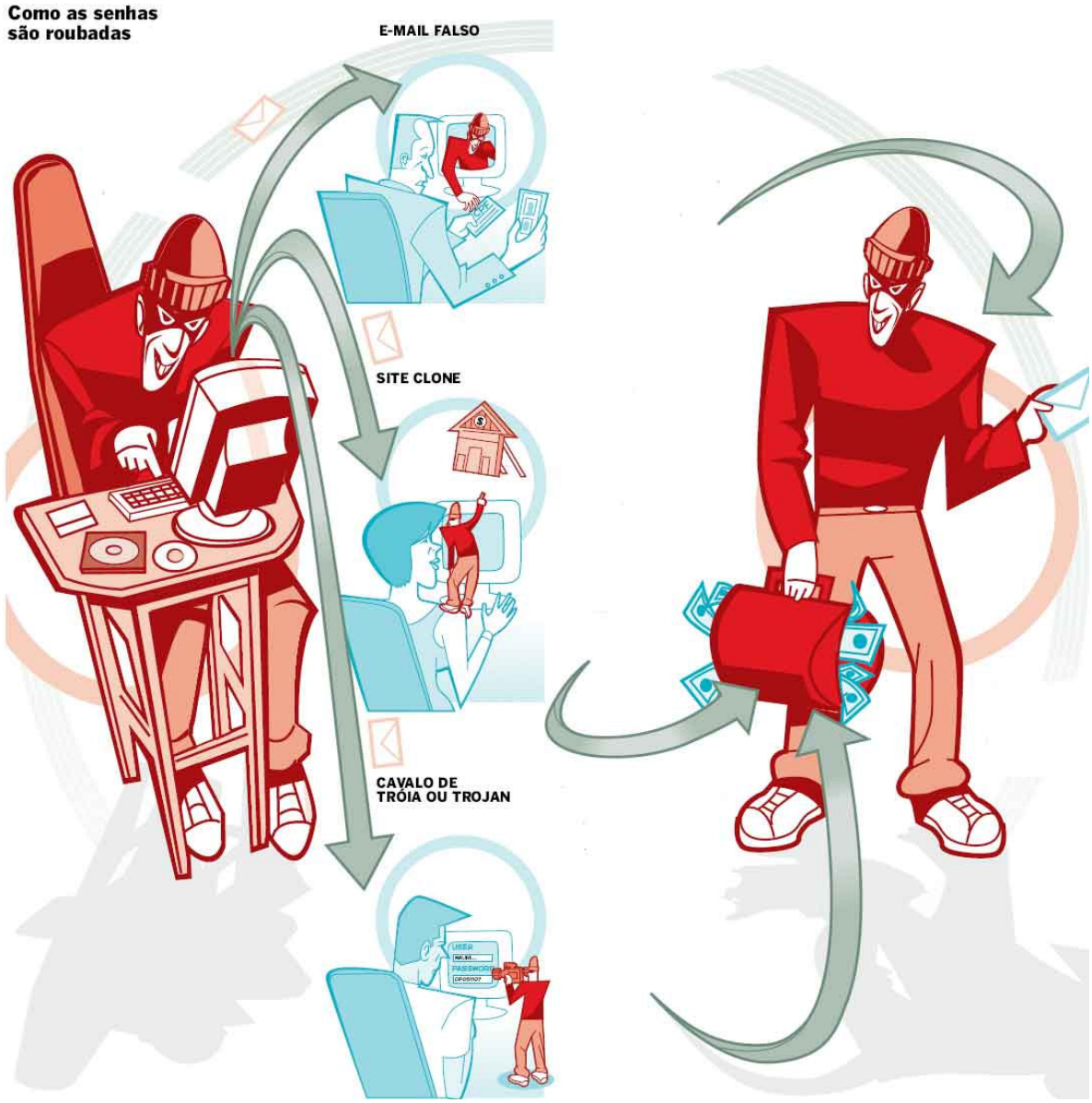


FIGURA 16: Imagem de exemplificação de Fraude na Internet (Fonte: Estado de São Paulo – Caderno LINK)

A informática hoje em dia não só permite isso como de certa maneira ainda incentiva estas ações, devido a impunidade que alastra os malfeitores virtuais, e também devido o fato da facilidade em se manter anonimato ou talvez até se utilizar de uma falsa identidade conseguida por meios não regulares. Mas da mesma maneira que a Internet possibilita esses tipos de delitos ela também pode impedir caso haja uma grande conscientização, os recursos hoje em dia disponíveis para empresas que queriam combater esses tipo de delitos são

grandes, tais como servidores Proxy, firewalls, pessoal especializado e outra gama de funções disponíveis.

Firewall é uma ferramenta que se corretamente utilizada ajuda a combater vários tipos de invasão, pois ele serve como uma proteção impedindo conexões suspeitas ou indesejadas, assim eliminando grande parte dos ataques de pessoas com pouco conhecimento mas más intenções.

Outra ferramenta que pode ser muito utilizada é o Anti-virus que pode ajudar a combater boa parte dos scams que acontecem pelo fato deles serem feitos por worms, assim sendo os antivírus podem detectar e eliminar esses programas mantendo o seus sistema o mais estável e seguro possível.

Uma outra ferramenta que muito colabora para a segurança da informação é a criptografia que nos permite ter acessos mais seguros e permite a informação trafegar com mais segurança, tendo em vista que a informação criptografada não consiguirá ser lida caso não seja descriptografada com a chave de criptografia adequada.

Outras maneiras de se manter a segurança de seu computador ou de sua informação é a conscientização dos usuários, ensinando-os a manter cópias de seguranças e tomarem cuidado com sites e e-mails suspeitos.

Para as empresas também há de recordar que um segurança física é tão importante quanto uma segurança virtual, pois as vezes uma invasão pode se originar de uma falha na segurança física do servidor.

3 PROPOSTA DE UM AMBIENTE ANTICRIME

No início deste trabalho havia a intenção de elaborar um software que ajudasse a prevenir ou ao menos diminuir os crimes virtuais anteriormente citados, mas não foi possível chegar a uma versão funcional. Assim, o trabalho teve um propósito investigativo e de análise dos possíveis problemas que podem vir a surgir.

O estudo mostrou, também, como tem sido complicada a computação de segurança acompanhar a velocidade com que os crimes ocorrem e evoluem. Mostrou, também, que geralmente os crimes virtuais ocorrem devido a falhas na máquina humana. Estudos pesquisados comprovaram que a maioria dos casos não se tratava apenas de uma falha no sistema computacional e sim a falta de ética e ingenuidade das pessoas. Muitas pessoas que usam diariamente um computador em seu trabalho ou residência são as principais responsáveis pela maior parte das fraudes devido à falta de informação, a inocência no uso da máquina, ou porque os dados de suas máquinas são coletados sem seu consentimento ou conhecimento.

Estes fatores dificultam, ainda, mais o trabalho de programadores que buscam uma maneira eficiente para evitar alguns tipos de crimes na Internet.

A partir destas constatações decidiu-se criar uma ferramenta que pudesse colaborar para diminuir este tipo de crime e evitar que o usuário tivesse seus dados roubados sem seu consentimento.

O software teria por objetivo verificar e evitar que pessoas fossem atraiçoadas por programas maliciosos que poderiam monitorar suas atividades enquanto no computador e, assim, repassar as suas informações para outras pessoas. Dessa forma, impedir que estas informações pudessem ser utilizadas para prejudicar a própria pessoa ou seu semelhante.

Para tal fim, foram pesquisadas diferentes maneiras como isto poderia ser feito.

As pesquisas mostraram que a solução poderia estar no Windows XP. A partir da verificação do diretório c:\Windows\Prefetch seria possível saber se alguma coisa havia sido alterada no sistema e se tinha algum programa rodando escondido nos bastidores do sistema.

A opção por este diretório ocorreu pelo fato do recurso prefetch do Windows XP carregar em sua memória os componentes mais utilizados pelos aplicativos, o que torna o boot e a abertura de programas mais rápidos. O diretório prefetch, também, contém um log que armazenam os componentes que foram mais utilizados e que têm preferência no carregamento. Assim um programa que monitoraria as ações do usuário no computador deveria estar neste diretório devido ao fato dele ser carregado no boot e se manter em funcionamento enquanto o computador permanece ligado. Esta seria uma boa maneira de manualmente o usuário procurar vestígios de invasão.

O programa monitoraria tal diretório e informaria ao usuário se algo anormal estivesse ocorrendo, e assim, o usuário poderia tomar as atitudes adequadas quanto ao acontecido. No entanto, esbarramos em alguns problemas. O programa não detectaria falhas caso antes de sua instalação já houvesse algum programa invasor instalado no computador do usuário, o que diminuía muito a sua eficiência.

Após, um estudo mais aprofundado descobriu-se outro inconveniente, este programa detectaria tudo como um invasor ou nada como invasor. Desta forma, teria apenas o caráter de informar ao usuário que algo novo foi encontrado no prefetch, mas o conteúdo encontrado no diretório só poderia ser analisado por alguém com um bom conhecimento em informática, o que restringia muito a eficácia do programa.

Após estas avaliações foi considerado que o programa não seria funcional e totalmente inviável de ser implementado.

Com base na pesquisa bibliográfica realizada e em toda a análise feita durante a elaboração da proposta para o desenvolvimento de um ambiente anticrime percebeu-se que a

forma mais eficiente para diminuir o número de crimes que aconteciam diariamente no mundo virtual seria a elaboração de um programa educativo para os usuários de computadores. Este programa teria como função conscientizar a população sobre os principais crimes virtuais e as formas corriqueiras para preveni-los.

Além de palestras educativas para o público interessado poderia ser desenvolvido um site de caráter informativo.

3.1. Programa amigável de verificação de invasões

Para fins de estudo foi-se desenvolvido o programa acima citado, onde o programa tem por objetivo monitorar o diretório prefetch em busca de vestígios de algum tipo de invasão no computador citado.

Este programa terá funcionalidade apenas em computadores que utilizem o Windows XP e que tenham sido recém formatados. O programa tem por finalidade apenas auxiliar a busca de vestígios de invasão de programas maliciosos.

O diretório prefetch é a essência do programa, tendo em vista que o Windows cria um arquivo .pf neste diretório para todo programa que seja executado na sua inicialização e para todo programa que seja freqüentemente usado.

Tendo em base o conhecimento acima citado o programa tem por finalidade verificar e avisar caso algum novo arquivo seja encontrado neste diretório, e caso o usuário não tenha feito nenhuma instalação recente este será um sinal para ele tomar cuidado pois seu sistema pode estar comprometido.

O Programa quando inicializado irá verificar se ele já possui uma lista dos arquivos do prefetch e caso este arquivo não exista ele irá criar com os arquivos que atualmente fazem parte do diretório prefetch.

```
public void criaRegistro(){
    File dir = new File("c:\\Windows\\Prefetch\\");
    String[] children = dir.list();
        try{
            BufferedWriter grava = new BufferedWriter(new
                                FileWriter("program2bd.txt",true));
            if (children == null) {
            } else {
                for (int i=0; i<children.length; i++) {
                //String filename = children[i];
                System.out.println(children[i].toString());
                grava.write(children[i].toString());
                grava.newLine();
                }
            grava.close();
            ArqSaida.append("Arquivo contendo os principais
                arquivos de prefetch do Windows\nfoi criado com Sucesso");
            }
        }catch(Exception e){};

}
```

No caso do Arquivo com a lista de arquivos do prefetch já existir o programa irá criar um vetor atualizado com todos os arquivos atualmente no diretório e um vetor com os arquivos já registrados na base de dados do programa.

```
public void criaVetor(){
    try{
        FileReader reader = new FileReader("program2bd.txt");
        BufferedReader leitor = new BufferedReader(reader);
        int l = 0;
        int numElem = contarLinhas();
        vetorTeste = new String[numElem];
        String s = "";
        while((s =leitor.readLine()) != null){
                vetorTeste[l]=s;
                l++;
            }
        ArqSaida.append("Vetor Criado com Sucesso");
        leitor.close();
        reader.close();
    }catch(Exception e){
        e.printStackTrace();
    }

}
```

Após ter sido criado os dois vetores o programa inicializará as comparações na busca de saber se existe algum arquivo no diretório prefetch o qual não esta registrado na base de dados. No caso de existir um arquivo novo o programa mostrará na tela que existe um novo arquivo, seu nome e perguntará se deseja adicionar o arquivo na base de dados. Lembrando que o programa lhe falará da existência do novo arquivo a atitude a ser tomada com relação a isso é do usuário. Caso ele tenha instalado recentemente um novo programa provavelmente esse novo arquivo seja relativo ao novo programa instalado, mas caso o sistema não tenha sido alterado nos ultimos dias esse é um forte indicio de um programa malicioso alojado em sua máquina.

3.2. Aspectos funcionais do programa

O programa aqui desenvolvido e citado funciona fazendo uma verificação dentro do diretório prefetch. Para o programa trazer algum resultado o usuário deverá rodá-lo pela primeira vez quando acabar de fazer a formatação completa de seu computador e tiver

instalado todos seus programas essenciais, assim sendo o programa criará uma lista dos arquivos que serão mais usados pelo windows e que são seguros. A partir daí todos os dias o usuário poderá rodar o programa em busca de saber se houve alguma alteração no funcionamento normal de sua máquina, pois caso apareça algo novo no diretório prefetch sem que o usuário tenha instalado este será um sinal de que existe algo errado. Por este motivo o usuário deverá, sempre que instalar um novo software, rodar o programa novamente para fim de atualizar sua lista de arquivos comumente executados e seguros do windows.

Para fim de testes foram adicionados, à mão, arquivos novos no diretório prefetch a fim de ver se o programa detectaria e avisaria seu usuário do acontecimento, em todas às vezes teve-se um resultado afirmativo.

No desenvolvimento do programa inicialmente foi-se buscar um algorítmo que fosse capaz de detectar mudanças no diretório prefetch, tendo em vista que este diretório cria um arquivo de registro para os componentes mais comumemte usados pelo windows XP, assim o windows XP usa esse log para fim de carregar esses componentes em memória fazendo com que o boot do computador seja mais eficiente. Tendo em vista essas informações foi percebido a possibilidade de se encontrar vestígios de invasão por meio desse diretório, pois quando um programa de invasão é alojado no computador ele será sempre executado, então o windows XP irá criar um arquivo para tal programa malicioso, deixando assim um traço para que possa se descobrir a invasão e assim tomar as atitudes necessárias. Antes do desenvolvimento desse trabalho já havia se descoberto essa possibilidade e na maioria das vezes se mostrando uma forma eficiente de procurar vestígios de invasão.

A partir do momento em que o código do programa foi criado, testado e simplificado ao máximo para buscar eficiência, agora será desenvolvida uma interface amigável para usuários leigos tenham acesso a tal programa. A interface conterá os botões de ação do programa como conterá também uma parte informativa para o usuário leigo entender o

funcionamento do programa e entender o que são os programas maliciosos do qual ele está buscando se defender.

CONCLUSÃO

Com o estudo realizado foi possível identificar que hoje em dia acontecem inúmeros tipos de crimes pela Internet, que antes só se era visto fora dela.

Com a implementação da proposta de um software anticrime, pode-se perceber que é se possível criar programas que auxiliem no combate contra os crimes na internet, mas de nada adiantará investir milhões em segurança se ao mesmo tempo não investirmos tempo e dinheiro na conscientização e treinamento de pessoal especializado.

O Software apesar de simples ele auxilia o combate de um certo tipo de crime, e pode ser aprimorado para assim se tornar mais usual e mais fácil ao usuário leigo de utilizá-lo.

Com o desenvolvimento deste este trabalho pode-se perceber que a Internet influenciou o aparecimento de novas formas crimes. Entre estes podem ser citados: pedofilia, fraudes, preconceito, danos morais, ofensa a honra. Fora todos esses pode-se também olhar mais a frente e analisar alguns tipos de crimes que se já existem, não foram ainda documentados, tais como: assassinato e terrorismo.

Desta forma, fatores como: o anonimato, a facilidade para se utilizar falsidade ideológica, a falta de uma constituição firme que condene alguns tipos de crime, resultaram em uma certa impunidade.

Estes e outros motivos impulsionaram o aparecimento de novos criminosos virtuais, que aqui também buscamos classificar alguns deles, tais como Hackers, Crackers, carders, entre outros.

Entre todos os tipos de crimes que se é possível classificar com este trabalho foi-se possível também ouvir rumores sobre alguns tipos de crimes que não foram expostos nesse trabalho devido a falta de informação, este crime seria o ciberterrorismo, pois se estamos na era da informação e a informação se encontra na internet países e governos podem ser

afetados por esses tipos de crimes, abrindo assim as possibilidades para este tipo de crime. Infelizmente as informações sobre isso eram excassas permitindo apenas citá-lo.

REFERÊNCIAS

ALMEIDA, A. V. Direito para todos. **Prodide em revista**, p.26-27, 2004.

ARRUDA, A. T. M. **A ética na relação profissional-paciente-família.** Marília: [S.N.], 2004.

BRASIL. Lei nº 10.764, de 12 de novembro de 2003. Altera a Lei nº 8.069, de 13 de julho de 1990, que dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 13 nov. 2003. p. 1.

BRASIL. Lei n. 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do artigo 5° da Constituição Federal. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 25 jul. 1996.

BRASIL. Código Penal (1940). Lei nº 9983, 14 de julho de 2000. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 17 jul. 2000.

BRASIL. Decreto nº 3.505 de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 14 jun de 2000. Seção 1 p. 2.

BRASIL. **Projeto de lei nº 84,** de 1999. Dispõe sobre os crimes cometidos na área de informática, suas penalidades, e dá outras providências. Disponível em <http://www.advogado.com/internet/84-99.htm>. Acesso em: 10 out. 2005

BRASIL. **Projeto de lei nº 4144, de 2004.** Altera a Lei nº 8.069, de 13 de julho de 1990, a Lei nº 9.296, de 24 de julho de 1996, e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, e dá outras providências. Disponível em <http://cbeji.com.br/br/novidades/legislacao/main.asp?id=3552>. Acesso em: 10 out. 2005

(CAIS, 2005) - **CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANÇA (CAIS).** Rede Nacional de Ensino e Pesquisa (RNP). Disponível em <http://www.rnp.br/cais/>. Acesso em: 29 de outubro de 2005.

CARTILHA DE SEGURANÇA PARA INTERNET. Disponível em <http://cartilha.cert.br/>. Acesso em: 7de setembro de 2005.

(CERT.BR, 2005) - CERT.br . **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.** Disponível em <http://www.cert.br/>. Acesso em: 29 de outubro de 2005.

CYBERCRIME CONVENTION, 2001. Computer Crime and Intellectual Property Section. Disponível em <http://www.usdoj.gov/criminal/cybercrime/intl.html#Vb1>. Acesso em: 29 de outubro de 2005

DE REZENDE, P. A. D. **Ciberterrorismo e guerra cognitiva**. Palestra de Abertura do III Congresso Internacional de Direito e Tecnologias da Informação, Bahia, 2004. Disponível em: <http://www.cic.unb.br/docentes/pedro/trabs/cibercon04.html>. Acesso em: maio, 2005.

FERREIRA, F N F. **O elo mais fraco da segurança: o fator humano.** Módulo Security Magazine, jul. 2005. Disponível em <http://www.modulo.com.br/>. Acesso em 01 agosto de 2005.

Folha de São Paulo on-line caderno dinheiro de 25/08/2004. Disponível em <http://www1.folha.uol.com.br/folha/dinheiro/ult91u99624.shtml>. Acesso em: 07 out. 2005.

GOMES, R. R. **Crimes puros de informática**. Brasília, [Trabalho de Conclusão de Curso em Direito - Centro Universitário de Brasília], 2001.

IMAGUIRE, G. **Ética e moral.** In: Filósofos, 2000. Disponível em: <http://www.filosofos.com.br/tema_etica.htm >. Acesso em: 10 out. 2005.

INTERNATIONAL DATA GROUP (IDG Brasil) **O Mercado TI e Telecom no Brasil.** Disponível em < http://www.idg.com.br/>. Acesso em 30 de setembro de 2005.

KANT, I. **Fundamentação da metafísica dos costumes.** Lisboa: Edições 70, 1997.

LICKS, O. B.; JUNIOR ARAÚJO, J. M Aspectos penais dos crimes de informática no Brasil. **Revista dos tribunais,** Rio Grande do Sul, 1994. p. 97.

MANZUR, C L. Chile: los delictos de hacking en sus diversas manifestaciones**. Revista Electrónica de Derecho Informático**, n. 21, Abril del 2000.

MARCHIONNI, A. **A ética e seus fundamentos**. IN: MARCÍLIO, M. L.; RAMOS, E. L. Ética na virada do milênio : busca do sentido da vida. São Paulo: LTR Editora, 1999.

MÓDULO SECURITY SOLUTIONS. **9ª Pesquisa Nacional de Segurança da Informação** Rio de Janeiro, 2003.

MOREIRA, S. N. **Segurança mínima**: uma visão coorporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001.

PINHEIRO, R C. Os cybercrimes na esfera jurídica brasileira . **Jus Navigandi**, Teresina, a. 4, n. 44, ago. 2000. Disponível em <http://jus2.uol.com.br/doutrina/texto.asp?id=1830>. Acesso em: 07 out. 2005

UNITED NATION STATISTICS DIVISION. **Millennium Indicators.** 2005. Disponível em <http://unstats.un.org/unsd/mi>. Acesso em: 10 de outubro de 2005.

(POLÍCIA FEDERAL, 2005) - **Agência de notícias da policia federal.** Disponível em <http://www.dpf.gov.br/DCS/>. Acesso em: 10 de outubro de 2005.

RODRIGUES, J R. S. **Crimes de informática e a legislação brasileira**. Minas Gerais, [Monografia do Curso de pós-graduação Lato Sensu em Administração de Redes Linux - Departamento de Ciência da Computação - da Universidade Federal de Lavras], 2004.

SÃO PAULO. Ministério Público. **Brasil está na rota dos crimes na Internet.** In: Agência Brasil, 2004. Disponível em <http://www.mp.sp.gov.br/Seguranca/altera/NoticiasAnteriores2004.htm>. Acesso em: 10 de outubro de 2005.

TURBAN, E.; KING, D**. Comércio eletrônico**: estratégia e gestão. São Paulo: Prentice Hall, 2004.

VASCONCELLOS, M. J. A. **A Internet e os hackers**: ataques e defesas. 5.ed. São Paulo: Chantal, 2000.

APÊNDICE

APÊNDICE A – Classe ProjetoJava

```
/*
 * ProjetoJava.java
 *
 * Criado em          : 9 de Março de 2005, 15:49
 * Ultima Modificação : 9 de Novembro de 2005, 18:03
 */

import java.io.*;
import java.util.*;
import java.util.StringTokenizer.*;
import javax.swing.*;
/**
 *
 * @autor  tiago
 */
public class projetojava extends javax.swing.JFrame {
        public String[] vetorTeste;

   /** Cria o Form */
        public projetojava() {

                super("Auxilio A combate de Invasões");
                initComponents();

   }



   private void initComponents() {//GEN-BEGIN:initComponents
                ArqSaida = new javax.swing.JTextArea();

      getContentPane().setLayout(null);

      addWindowListener(new java.awt.event.WindowAdapter() {
         public void windowClosing(java.awt.event.WindowEvent evt) {
            exitForm(evt);
         }
      });
```

```
        ArqSaida.setEditable(false);
        getContentPane().add(ArqSaida);
        ArqSaida.setBounds(10, 30, 380, 260);

        pack();
    }//GEN-END:initComponents

    /** Exit the Application */
    private void exitForm(java.awt.event.WindowEvent evt) {//GEN-FIRST:event_exitForm
        System.exit(0);
    }//GEN-LAST:event_exitForm

        public int contarLinhas(){
                int count=0;
                try{
                        FileReader reader = new FileReader("program2bd.txt");
                        BufferedReader contador = new BufferedReader(reader);
                        while((contador.readLine())!= null){
                                count++;
                        }
                        reader.close();
                        contador.close();
                }catch(Exception e){
                        e.printStackTrace();
                }
                return count;
        }

        public void criaRegistro(){
                File dir = new File("c:\\Windows\\Prefetch\\");
                String[] children = dir.list();
                        try{
                                BufferedWriter grava = new BufferedWriter(new
FileWriter("program2bd.txt",true));
                        if (children == null) {
                        } else {
                           for (int i=0; i<children.length; i++) {
                                        System.out.println(children[i].toString());
                                        grava.write(children[i].toString());
                                        grava.newLine();
                        }
                                grava.close();
                                ArqSaida.append("Arquivo contendo os principais arquivos de
prefetch do Windows\nfoi criado com Sucesso");
                        }
                        }catch(Exception e){};

        }
```

```
	public void criaVetor(){
		try{
			FileReader reader = new FileReader("program2bd.txt");
			BufferedReader leitor = new BufferedReader(reader);
			int l = 0;
			int numElem = contarLinhas();
			vetorTeste = new String[numElem];
			String s = "";
			while((s =leitor.readLine()) != null){
					vetorTeste[l]=s;
					l++;
				}
			ArqSaida.append("Vetor Criado com Sucesso");
			leitor.close();
			reader.close();
		}catch(Exception e){
			e.printStackTrace();
		}

	}



	public void verificaRegistro(){

      File dir = new File("c:\\Windows\\Prefetch\\");
		String[] children = dir.list();
		criaVetor();
		ArqSaida.append("\nInicializando o Teste... Por Favor Aguarde...");
		int verificador = 0;
		boolean flag = false;
		for (int i=0; i<children.length; i++) {
			verificador = 0;
			for(int f = 0; f < contarLinhas(); f++){
				if(children[i].equals(vetorTeste[f])){
					verificador = 1;
				}
			}
			if(verificador == 0){
				flag = true;
				ArqSaida.append("\n\n************************
ATENÇÃO    ************************");
				ArqSaida.append("\nO arquivo "+ children[i] +" não foi
encontrado\nna base de dados!!! Favor verificar!!!");
				if(	(JOptionPane.showConfirmDialog(null, "Deseja
Adicionar o Arquivo à base de dados?","Novo Arquivo Encontrado" ,
JOptionPane.YES_NO_OPTION) )== 0)
```

```
                                        {
                                                adicionaRegistro(children[i]);
                                        }
                                }
                        }
                        if(!flag){
                                ArqSaida.append("\n\n\t>>> Verificação Concluída  <<<\n\tNenhum
Arquivo Novo Encontrado!!!");
                        }
        }

        public void adicionaRegistro(String arquivoNovo){
                try{
                        BufferedWriter grava = new BufferedWriter(new
FileWriter("program2bd.txt",true));
                        grava.write(arquivoNovo);
                        grava.close();
                        ArqSaida.append("\n\n>>>>>Arquivo Adicionado!<<<<<");
                }catch(Exception e){};

        }



   public static void main(String args[]) {
      projetojava programa = new projetojava();
                programa.setSize(410,330);
                programa.show();

                File teste = new File("program2bd.txt");
                if(teste.exists()){

                        programa.verificaRegistro();



/*
                Caso Não exista o arquivo ainda ele cria o arquivo por base em todos os
programas que estiverem registrados no prefetch
*/
                }else{

                        programa.criaRegistro();

                }
   }



   // Variables declaration - do not modify//GEN-BEGIN:variables
```

```
    javax.swing.JTextArea ArqSaida;
    // End of variables declaration//GEN-END:variables

}
```

ANEXO

ANEXO A – Projeto de Lei Nº84/99

PROJETO DE LEI Nº 84/99

Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.

O Congresso Nacional decreta:

CAPÍTULO I

DOS PRINCÍPIOS QUE REGULAM A PRESTAÇAO DE SERVIÇO POR REDES DE COMPUTADORES

Art. 1º - O acesso, o processamento e a disseminação de informações através das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede.

Art. 2º - É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições específicas reguladas em lei.

CAPÍTULO II

DO USO DE INFORMAÇÕES DISPONÍVEIS EM COMPUTADORES OU REDES DE COMPUTADORES.
Art. 3º - Para fins desta lei, entende-se por informações privadas aquelas relativas a pessoa física ou jurídica identificada ou identificável.

Parágrafo único. É identificável a pessoa cuja individuação não envolva custos ou prazos desproporcionados.

Art. 4º - Ninguém será obrigado a fornecer informações sobre sua pessoa ou de terceiros, salvo nos casos previstos em lei.

Art. 5º - A coleta, o processamento e a distribuição, com finalidades comerciais, de informações privadas ficam sujeitas à prévia aquiescência da pessoa a que se referem, que poderá ser tomada sem efeito a qualquer momento, ressalvando-se o pagamento de indenizações a terceiros, quando couberem.
§ 1º. A toda pessoa cadastrada dar-se-á conhecimento das informações privadas armazenadas e das respectivas fontes.
§ 2º. Fica assegurado o direito à retificação de qualquer informação privada incorreta.

§ 3º. Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação privada será mantida à revelia da pessoa a que se refere ou além do tempo previsto para a sua validade.
§ 4º. Qualquer pessoa, física ou jurídica, tem o direito de interpelar o proprietário de rede de computadores ou provedor de serviço para saber se mantém informações a seu respeito, e o respectivo teor.

Art. 6º - Os serviços de informações ou de acesso a bancos de dados não distribuirão informações privadas referentes, direta ou indiretamente, a origem racial, opinião política, filosófica, religiosa ou de orientação sexual, e de filiação a qualquer entidade, pública ou privada, salvo autorização expressa do interessado.

Art. 7º - O acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores dependerá de prévia autorização judicial.

CAPÍTULO III

DOS CRIMES DE INFORMÁTICA

Seção I
Dano a dado ou programa de computador

Art. 8º - Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Parágrafo único. Se o crime é cometido:

I - contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II- com considerável prejuízo para a vítima;
III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV - com abuso de confiança;
V - por motivo fútil;
VI - com o uso indevido de senha ou processo de identificação de terceiro , ou
VII - com a utilização de qualquer outro meio fraudulento.
Pena: detenção, de dois a quatro anos e multa.

Seção II
Acesso indevido ou não autorizado

Art. 9º Obter acesso, indevido ou não autorizado, a computador ou rede de computadores.

Pena: detenção, de seis meses a um ano e multa.

Parágrafo primeiro. Na mesma pena incorre quem. sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.

Parágrafo segundo. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II - com considerável prejuízo para a vítima;
III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV - com abuso de confiança;
V - por motivo fútil;
VI - com o uso indevido de senha ou processo de identificação de terceiro; ou
VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção III
Alteração de senha ou mecanismo de acesso a programa de computador ou dados

Art. 10. Apagar, destruir, alterar, ou de qualquer fama inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.

Pena: detenção, de um a dois anos e multa.

Seção IV
Obtenção indevida ou não autorizada de dado ou instrução de computador

Art. 11. Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador.
Pena: detenção, de três meses a um ano e multa.

Parágrafo Único. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II - com considerável prejuízo para a vítima;
Parágrafo Único. Se o crime é cometido:
I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II - com considerável prejuízo para a vítima;
III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV - com abuso de confiança;
V - por motivo fútil;
VI - com o uso indevido de senha ou processo de identificação de terceiro; ou
VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção V
Violação de segredo armazenado em computador, meio magnético, de natureza magnética, óptica ou similar

Art. 12. Obter segredos, de indústria ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Seção VI
Criação, desenvolvimento ou inserção em computador de dados ou programa de computador c nocivos

Art. 13. Criar, desenvolver ou inserir, dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.

Pena: reclusão, de um a quatro anos e multa.

Parágrafo único. Se o crime é cometido:

I - contra a interesse da União, Estado, Distrito Federal. Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II - com considerável prejuízo para a vítima;
III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV - com abuso de confiança;
V - por motivo fútil;
VI - com o uso indevid6 de senha ou processo de Identificação de terceiro; ou
VII - com a utilização de qualquer outro meto fraudulento.

Pena: reclusão, de dois a seis anos e multa.

Seção VII
Veiculação de pornografia através de rede de computadores

Art. 14. Oferecer serviço ou informação de caráter pornográfico, em rede de computadores, sem exibir, previamente, de forma facilmente visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para criança ou adolescentes.

Pena: detenção, de um a três anos e multa.

CAPITULO IV

DAS DISPOSIÇÕES FINAIS

Art. 15. Se qualquer dos crimes previstos nesta lei é praticado no exercício de atividade profissional ou funcional, a pena é aumentada de um sexto até a metade.

Art. 16. Nos crimes definidos nesta lei somente se procede mediante representação do ofendido, salvo se cometidos contra o interesse da União, Estado, Distrito Federal Município, órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundações instituídas ou mantidas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresas que explorem ramo de atividade controlada pelo poder público, casos em que a ação é pública incondicionada.

Art. 17. Esta lei regula os crimes relativos à informática sem prejuízo das demais comunicações previstas em outros diplomas legais.

Art 18. Esta lei entra em vigor 30 (trinta) dias a contar da data de sua publicação.

Deputado LUIZ PIAUHYLINO

ANEXO B – Convenção em Cibercrimes

CONVENTION ON CYBERCRIME

Budapest, 23.XI.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data;

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party’s international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of

efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its

domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

– the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

– the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

– the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.