UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS V
CENTRO DE CIÊNCIAS BIOLÓGICAS E SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

ARTUR OLIVEIRA ARAÚJO

COOPERAÇÃO INTERNACIONAL CONTRA O CIBERCRIME: a importância dos países em desenvolvimento.

JOÃO PESSOA – PB
2010

UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS V
CENTRO DE CIÊNCIAS BIOLÓGICAS E SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

ARTUR OLIVEIRA ARAÚJO

COOPERAÇÃO INTERNACIONAL CONTRA O CIBERCRIME: a importância dos países em desenvolvimento.

JOÃO PESSOA – PB
2010

ARTUR OLIVEIRA ARAÚJO

COOPERAÇÃO INTERNACIONAL CONTRA O CIBERCRIME: a importância dos países em desenvolvimento.

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Relações Internacionais da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Bacharel.

Orientadora: Profª Drª Luiza Rosa Barbosa de Lima

JOÃO PESSOA – PB
2010

F ICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA SETORIAL CAMPUS V – UEPB

A663c Araujo, Artur Oliveira.
Cooperação internacional contra o cibercrime: a importância dos países em desenvolvimento / Artur Oliveira Araujo. – 2010.
40f. : il. color.

Digitado.
Trabalho Acadêmico Orientado (Graduação em Relações Internacionais) – Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas, 2010.
"Orientação: Profª. Dra. Luiza Rosa Barbosa de Lima".

1. Cibercrime. 2. Cooperação Internacional. 3. Tecnologia da Informação e Comunicação I. Título.

21. ed. CDD 327.17

UNIVERSIDADE ESTADUAL DA PARAÍBA

CURSO DE BACHARELADO EM RELAÇÕES INTERNACIONAIS

FOLHA DE DEFESA COM OS MEMBROS DA BANCA

ALUNO(A): ARTUR OLIVEIRA ARAUJO
MATRÍCULA: 07152065-1

COOPERAÇÃO INTERNACIONAL CONTRA O CIBERCRIME: a importância dos países em desenvolvimento.

Monografia apresentada ao Curso de Relações Internacionais da Universidade Estadual da Paraíba.

Professor(a) Luiza Rosa Barbosa de Lima (Orientador(a)) - UEPB

Professor(a) Messias Rafael Batista - UEPB

Professor(a) Anahi de Castro Barbosa - UEPB

João Pessoa , 02 de dezembro de 2010.

RESUMO

O surgimento da internet e das tecnologias da informação proporcionaram maior velocidade na troca de informações no mundo moderno, as instituições passaram a usar desse mundo virtual para organizar-se e melhor atender a demanda da sociedade moderna. No entanto, a internet proporciona também um espaço livre de regras e leis onde o usuário de um computador localizado em qualquer lugar do mundo pode influenciar a rede inteira com suas ações, essa propriedade da rede se torna uma arma na mão de criminosos, facilitando crimes já existentes e dando origem a novos tipos de crimes. À medida que a prática do crime é facilitada, seu combate é dificultado, torna-se necessário o surgimento de novas formas de combate sejam elas técnicas, no que se refere a investigações, ou legais. Devido à natureza transnacional do crime, os países em desenvolvimento são os principais causadores e vítimas dos crimes virtuais devido à falta de técnicas e medidas para combatê-los. Dessa forma, algumas medidas para prevenção dos crimes tornam-se inviáveis devido a falta de instrumentos para este fim. Logo, devido a importância desses países para perseguir os criminosos, a cooperação internacional é arma primordial ao seu desenvolvimento no combate ao cibercrime.

PALAVRAS-CHAVE: Cibercrime. Cooperação Internacional. Tecnologias da informação e comunicação. *Safe havens*.

ABSTRACT

The emergence of the Internet and information technology provided a higher speed for information exchange in the modern world, the institutions began to use this virtual world to organize themselves and better meet the demands of modern society. However the Internet also provides a space free of rules and laws where the user of a computer located anywhere in the world can influence the entire network with their actions, this property of the network becomes a weapon in the hands of criminals, facilitating existing crimes and creating new types of crimes. As the crime is facilitated, the combat is even more difficult, it is necessary the emergence of new ways to combat these crimes whether they are technical, with regard to investigations, or legal. Due to the nature of transnational crime, developing countries are primarily causes and victims of virtual crimes due to lack of techniques and measures to combat them. Thus, some measures for prevention of crimes become unviable due to lack of instruments for this purpose. Therefore, given the importance of these countries to pursue criminals, international cooperation is vital to their development weapon in fighting cybercrime.

KEYWORDS: Cybercrime. International Cooperation. Information and communications technology. Safe havens.

LISTA DE GRÁFICOS

LISTA DE SIGLAS

AGC	Agenda Global de Cibersegurança
DoS	Denial of Service
IGF	Internet Governance Forum
ONU	Organização das Nações Unidas
TIC	Tecnologias de Informação e Comunicação
UIT	União Internacional de Telecomunicações
UNCTAD	United Nations Conference on Trade and Development
VoIP	Voice over Internet Protocol

SUMÁRIO

INTRODUÇÃO

O surgimento das novas tecnologias da informação e comunicação, na segunda metade do século passado, que partiu da chamada revolução da informática e produziu a revolução digital, levou-nos ao aparecimento de uma nova sociedade: a Sociedade da Informação. Essa revolução digital que gerou a Sociedade da Informação surgiu modificando nossas vidas que vão sendo permeadas por redes e mecanismos digitais que adquiriram grande importância no funcionamento da sociedade atual. Com a criação da Internet todos passam a conectar-se e a globalização se acentua, pois essa rede internacional possibilita que pessoas de diferentes países, que antes dificilmente poderiam manter contato, possam trocar informações com maior velocidade.

As tecnologias da informação e comunicação (TIC), além de organizar a troca de informações, também servem para automação de mecanismos e são extremamente importantes para o funcionamento seja de serviços básicos da sociedade, como distribuição elétrica e hidráulica, seja para o funcionamento de empresas e órgãos dos governos, e até mesmo no fortalecimento tático militar.

> Many everyday communications depend on ICTs and Internet-based services, including VoIP calls or e-mail communications. ICTs are now responsible for the control and management functions in buildings, cars and aviation services. The supply of energy, water and communication services depend on ICTs. The further integration of ICTs into everyday life is likely to continue.[1] (GERCKE, 2009, p.64).

As TIC proporcionam uma evolução no modo de desenvolvimento, inserindo a humanidade numa nova era chamada a era da informação. A nova era apóia-se no modo de desenvolvimento informacional, em que as tecnologias que geram conhecimento, informação e comunicação são a fonte da produtividade. Apesar dos antigos modos de desenvolvimento basearem-se num certo grau de conhecimento, apenas no modo informacional o conhecimento age sobre os próprios conhecimentos proporcionando uma fonte de produtividade.

[1] Muitas comunicações diárias dependem de TIC e serviços baseados na Internet, incluindo as chamadas VoIP ou comunicações de e-mail. As TIC são responsáveis pelas funções de controle e gestão dos edifícios, automóveis e serviços de aviação. O fornecimento de energia, água e serviços de comunicações dependem das TICs. A maior integração das TIC na vida quotidiana é provável que continue.

> Assim, no modo agrário de desenvolvimento, a fonte do incremento de excedente resulta dos aumentos quantitativos de mão de obra e dos recursos naturais (em particular a terra) no processo produtivo, bem como da dotação natural desses recursos. No modo de desenvolvimento industrial, a principal fonte de produtividade reside na introdução de novas fontes de energia e na capacidade de descentralização do uso de energia ao longo dos processos produtivos e de circulação. No novo modo informacional de desenvolvimento, a fonte da produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos. Na verdade, conhecimento e informação são elementos cruciais em todos os modos de desenvolvimento, visto que o processo produtivo sempre se baseia em algum grau de conhecimento e no processamento da informação. Contudo, o que é específico ao modo informacional de desenvolvimento é a ação de conhecimentos sobre os próprios conhecimentos como principal fonte de produtividade. (CASTELLS, 2007, p.53).

No entanto com o surgimento da internet surge também um ambiente virtual de troca de informações onde os indivíduos são livres para ir e vir, no ambiente virtual não existem fronteiras nem mesmo autoridades com capacidade de regular e impor regras ou leis. Isso ocorre devido à própria natureza da internet, que a principio era usada para fins militares e necessitava de independência de qualquer centro de comunicação, a fim de dificultar a sua derrubada pelo inimigo. (ROSSINI, 2004, p.25-29)

> Com base na tecnologia de comunicação de troca de pacotes, o sistema tornava a rede independente de centros de comando e controle, para que a mensagem procurasse suas próprias rotas ao longo da rede, sendo remontada para voltar e ter sentido coerente em qualquer ponto da rede. (CASTELLS, 2007, p.82).

Dessa forma, esse ambiente se torna também um grande aliado de criminosos que procuram se aproveitar dessa troca de informações, ou ainda manipular informações de vital importância para órgãos do governo ou empresas a fim de arrecadar fundos ou criar oportunidades para pratica de crimes reais. Na era da informação, é quase impossível bloquear o fluxo de informações e à medida que a propriedade se torna digital, fruto de transações financeiras que passam a ocorrer nesse meio, essa também é transferida de forma livre tornando-as um alvo em potencial.

O presente trabalho busca analisar como a cooperação internacional pode influenciar esse tipo de crime, analisando dessa forma quais tipos de cooperação estão presentes neste cenário e como elas se comportam, de forma a ter uma maior compreensão do papel dos atores internacionais, em especial os países em desenvolvimento, no combate ao cibercrime. Para isso é necessário definir cibercrime e suas dinâmicas, de modo a facilitar a compreensão

sobre o tema, para em seguida explanar sobre as abordagens internacionais que buscam solucioná-lo.

Para fins da pesquisa foram analisados documentos oficiais de algumas das organizações internacionais mais relevantes para se tratar do tema juntamente com notícias dos principais jornais e meios de comunicação do mundo como o BBC, The New York Times e o Washington Post assim como outros meios mais técnicos como o Computer Weekly e o Information Week, com um recorte temporal de 2000 até os dias atuais. Neste trabalho são usados dados trabalhados pelo Dr. Marco Gercke e disponibilizados pela UIT através da obra "Understanding cybercrime: a guide for developing countries" analisados a luz das principais obras de Relações Internacionais que abordam os temas da sociedade atual e os adventos da globalização de Manuel Castells e os Tofflers, assim como cooperação internacional de Wladimir Valler Filho e organizações internacionais de Mônica Herz e Andrea Ribeiro Hoffmann trabalhando os conceitos e chegando a conclusões de forma dedutiva.

1. ENTENDENDO CIBERCRIME: CONSIDERAÇÕES GERAIS

De acordo com a Convenção sobre Cibercrime, cibercrime ou e-crime é um termo usado para se referir a todos os crimes que são cometidos através de redes de computadores, principalmente através da Internet. Este tipo de crime pode causar tanto danos materiais como morais, como ataque à pessoa como forma de violação aos direitos humanos. O cibercrime geralmente caracteriza-se como crimes cometidos através de redes de computadores que podem ou não apresentar particularidades desse meio. Em alguns casos as redes de computadores são usadas como um meio pelo qual serão praticados crimes reais, que em sua maioria já estão tipificados, em outros casos esses crimes são realizados de forma a afetar as TICs do qual a sociedade atual depende, causando perdas reais, essas raramente são tipificadas. Esse tipo de crime apresenta uma nova dinâmica aos crimes realizados, os criminosos agora não precisam se expor nem se arriscar tanto para conseguir seu objetivo. Em um ambiente como a internet, onde as fronteiras são inexistentes e sua identidade dificilmente é determinada, a prática de atos ilícitos é facilitada.

A escolha por esse espaço virtual não é ocasional, ele possibilita que o criminoso realize o crime sem correr riscos, pois a identificação do próprio se torna extremamente difícil, uma vez que o ataque se origina pela rede onde não se encontram autoridades fiscais ou reguladoras. A dificuldade na identificação não é o único e nem mesmo o maior dos problemas tratando-se de crimes virtuais, ainda que o criminoso seja identificado ele poderia estar situado em qualquer lugar do planeta, impossibilitando que o mesmo seja levado à justiça. Por isso quase sempre um crime virtual é também uma ocorrência internacional e merece atenção especial aos olhos das leis.

> Criminals need not be present at the same location as the target. As the location of the criminal can be completely different from the crime site, many cyber-offences are transnational. International cybercrime offences take considerable effort and time. Cybercriminals seek to avoid countries with strong cybercrime legislation.[2] (GERCKE, 2009, p.71).

[2] Os criminosos não precisam estar presentes no mesmo local que a vítima. A localização do criminoso pode ser completamente diferente do local do crime, muitas ciber-ofensas são transnacionais. Infrações internacionais sobre cibercrime necessitam de tempo e esforços consideráveis. Os cibercriminosos procuram evitar países com legislação forte sobre cibercrime.

Ao mesmo tempo em que os atos criminosos são facilitados a ação policial e a aplicação da lei é extremamente dificultada, pois os crimes agora ultrapassam as fronteiras dos estados, a resolução de apenas um crime pode envolver leis de até cinco Estados diferentes.

> Um americano recebe um falso e-mail com um link de fotos de uma brasileira. A mensagem direciona este usuário para um site brasileiro em português, que está, na verdade, roubando os dados deste usuário. Mas o servidor desta mensagem não está no Brasil, e sim na Rússia, onde disparar mensagens eletrônicas não desejadas pode não ser crime. É desta complexidade que estamos falando. Se não trabalharmos com um mínimo de cooperação, a tendência é o fracasso. (DANTAS, 2010).

Os atos ilícitos praticados através da internet exigem do usuário que está susceptível a tais crimes certo grau conhecimento técnico para que possa se proteger, a falta de conhecimento facilita ainda mais o trabalho do cibercriminoso. Esse tipo de crime pode ter como alvo tanto uma pessoa física como jurídica e até mesmos países inteiros. No caso do Brasil, o combate ao cibercrime ainda é fraco devido a dificuldades para estabelecer leis, sendo assim um dos maiores *safe havens* do mundo (ÂNGELO, 2002), servindo de moradia para muitos criminosos devido a impunidade. Apesar de todas essas características ainda é difícil chegar a um acordo sobre o que seria caracterizado como cibercrime.

> 21. There has been a great deal of debate among experts on just what constitutes a computer crime or a computer-related crime. Even after several years, there is no internationally recognized definition of those terms. […] There is no doubt among the authors and experts who have attempted to arrive at definitions of computer crime that the phenomenon exists. [...] A global definition of computer crime has not been achieved; rather, functional definitions have been the norm.[3] (UNITED NATIONS, 1994)

A Convenção sobre Cibercrime é o maior e mais respeitado documento internacional para debater o cibercrime. Essa prevê algumas formas pelos quais podemos classificar crimes virtuais através das possíveis infrações a serem cometidas.

[3] Há um grande debate entre especialistas sobre o que constitui um crime de computador ou um crime de informática. Mesmo depois de vários anos, não existe uma definição internacionalmente reconhecida de tais termos. [...] Não há dúvida entre os autores e especialistas que têm tentado chegar a definições de crime informático que o fenômeno existe. [...] Uma definição global da criminalidade informática não foi alcançada, mas sim, definições funcionais.

> 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.[4] (COUNCIL OF EUROPE, 2010)

Desta forma a convenção prevê crimes virtuais como sendo, ações direcionadas contra a confidencialidade, integridade e disponibilidade de sistemas, redes e dados de computador, assim como o mal uso dos mesmos. Para melhor ilustrar a definição da convenção disserta-se sobre possíveis ofensas a serem cometidas e classificadas como cibercrime.

1.1. Possíveis Ofensas no Meio Virtual

Ao falar de crimes no meio virtual a principal figura que vem a mente é a do cracker (erroneamente chamado de hacker). O cracker[5] é responsável pelo acesso indevido a redes de computadores, através do acesso ele pode obter informações importantes de uma empresa ou indivíduo a fim de manipular essas informações da forma como bem desejar. Nem sempre essas ações resultam em ganho para o cracker, mas quase sempre resultam em perda para quem é atacado. As principais ofensas que podem resultar dessa pratica são a alteração de informações, a venda de informações vitais (espionagem de dados) o desaparecimento de dados.

> Computer data are vital for private users, businesses and administrations, all of which depend on the integrity and availability of data. Lack of access to data can result in considerable (financial) damage. Offenders can violate the integrity of data and interfere with them by:
> • Deleting data; and/or

[4] Convencidos de que a presente Convenção é necessária para impedir os atos contra a confidencialidade, integridade e disponibilidade de sistemas, redes e dados informáticos, bem como o uso indevido de tais sistemas, redes e dados, prevendo a criminalização de tal conduta, conforme descrito na presente Convenção, e a adoção de poderes suficientes para combater eficazmente a tais delitos, facilitando a sua detecção, investigação e repressão, tanto a nível nacional e internacional e fornecendo mecanismos para uma rápida e confiável cooperação internacional.

[5] Crackers: são os verdadeiros criminosos virtuais. Diferente de um Hacker, que em princípio não é um criminoso, mas um especialistas em informática que procuram defeitos (bugs) nos sistemas operacionais e programas; Quando os descobrem, comunicam aos fabricantes e a toda a comunidade interessada, através de informativos periódicos, lista de discussão, etc. Os cracker são movidos por outros motivos e quando descobrem vulnerabilidades em sistemas informáticos, aproveitam-se dessas para causar danos, roubando, pichando, destruindo, etc.

- Suppressing data; and/or
- Altering data; and/or
- Restricting access to them.[6] (GERCKE, 2009, p.27).

O cracker também pode adquirir informações aproveitando-se da falta de informação dos usuários comuns, sem nem mesmo precisar invadir o computador. Uma pratica muito associada a isso é o chamado *phishing*, está geralmente associado ao envio de e-mails a fim de enganar os usuários menos atentos e está ligado a prática do spam. Através do *phishing* o cracker adquiri informações sobre o usuário, como numero de cartões de credito, CPF e outras informações vitais para prática de crimes reais.

Outra prática comum tem como alvo sistema de computadores ao invés de dados, muitas empresas disponibilizam serviços através da internet como parte de suas atividades, esses serviços estão susceptíveis a ataques que podem prejudicar os ganhos da empresa. Os artifícios mais usados para prática desse tipo de crime são os *worms* e os ataques DoS (Denial of Service). Os *worms* são programas de computador similares a vírus, que buscam afetar o sistema inteiro fazendo com que o seu desempenho seja comprometido. Os ataques DoS fazem com que os serviços disponibilizados pela empresa sejam comprometidos, impossibilitando o acesso pelos clientes. Esse tipo de ataque está associado ao uso de *botnets*, que são redes de computadores controlados remotamente pelo agressor, essas redes podem ser controladas através da internet e por apenas uma pessoa.

As ofensas também podem ser associadas à disponibilidade de dados, a internet é uma rede livre e possibilita a troca de material que pode ser considerado crime. Essa prática está geralmente associada à disponibilidade de material inadequado ou impróprio para menores, ou ainda a propagação de arquivos e sites de pedofilia ou que suportam a xenofobia, ferindo assim os direitos humanos, considerados universais e defendidos também pela Convenção sobre Cibercrime. Além dessas práticas, a disponibilidade de dados pode está associada à troca de material legal sem a devida autorização do autor (comumente conhecida como pirataria). A pirataria de dados é muito comum na rede e difícil de ser combatida, pelo fato de não ter um centro de operações, os arquivos são trocados entre os usuários num sistema que não necessita de um servidor central.

[6] Dados de computador são vitais para usuários particulares, empresas e administrações, as quais dependem da integridade e disponibilidade dos dados. Falta de acesso aos dados pode resultar em danos (financeiros) consideráveis. Infratores podem violar a integridade dos dados e interferir com eles: Excluindo dados e / ou; Eliminando dados e / ou; Alterando dados e / ou; Restringindo o acesso a eles.

> The technology used for file-sharing services is highly sophisticated and enables the exchange of large files in short periods of time. First-generation file-sharing systems depended on a central server, enabling law enforcement agencies to act against illegal file-sharing in the Napster network. Unlike first-generation systems (especially the famous service Napster), second-generation file-sharing systems are no longer based on a central server providing a list of files available between users. The decentralised concept of second-generation file-sharing networks makes it more difficult to prevent them from operating.[7] (GERCKE, 2009, p.42).

Também existem fraudes por meio de sistemas de computador, uma delas acontece por meio de sites de leilões e vendas de mercadorias, são muitos os sites que funcionam como intermediadores de negociações virtuais. O criminoso pode agir como comprador ou vendedor, vendendo sem o intuito de entregar o produto ou comprando sem o intuito de pagar, isso se dá pelo fato das negociações não serem feitas de forma presencial. Outra forma de fraude é a distribuição de e-mails em spam, requisitando o depósito de uma quantia em adiantamento para receber determinada premiação, esses e-mails são enviados de forma a convencer o usuário de que esse teria sido premiado, mas que para adquirir o prêmio teria que depositar valores em contas de terceiros relativos a custos administrativos.

Existem também formas de crime que tem como alvo o roubo ou a forja de documentos. Documentos eletrônicos são facilmente manipulados por esses criminosos e esse é exatamente um dos crimes que podem ser cometidos, a forja ou modificação de documentos eletrônicos possibilita ao criminoso enganar o usuário com mais facilidade, fazendo se passar por uma empresa ou outro usuário. Já o roubo de identidade consiste no uso de informações obtidas através de qualquer prática citada anteriormente para realizar ações criminosas no nome de outras pessoas ou vendendo seus dados para os mesmos fins.

> In general the offence described as identity theft contains three different phases:
> • In the first phase the offender obtains identity-related information. This part of the offence can for example be carried out by using malicious software or phishing attacks.

[7] A tecnologia utilizada para os serviços de compartilhamento de arquivos é altamente sofisticada e permite a troca de arquivos grandes em curtos períodos de tempo. A primeira geração de sistemas de compartilhamento de arquivos dependia de um servidor central, permitindo que as agências de aplicação da lei agissem contra o compartilhamento ilegal de ficheiros na rede Napster. Ao contrário da primeira geração de sistemas (especialmente o famoso serviço Napster), a segunda geração de sistemas de compartilhamento de arquivos já não se baseia em um servidor central que disponibiliza uma lista de arquivos disponíveis entre os usuários. O conceito de descentralização da segunda geração de redes de compartilhamento de arquivos torna mais difícil impedir seu funcionamento.

> • The second phase is characterised by interaction with identity-related information prior to the use of those information within criminal offences. An example is the sale of identity-related information. Credit card records are for example sold for up to 60 US dollars.
> • The third phase is the use of the identity-related information in relation with a criminal offence. In most cases the access to identity-related data enables the perpetrator to commit further crimes. The perpetrators are therefore not focusing on the set of data itself but the ability to use them in criminal activities. Examples for such offence can be the falsification of identification documents or credit card fraud.[8] (GERCKE, 2009, p.48).

Visto esses fatores, torna-se necessário entender as dificuldades de combater crimes virtuais para compreender a necessidade da cooperação entre os países ao tratar-se do combate a cibercrimes.

[8] Em geral, o delito descrito como roubo de identidade contém três fases distintas:
• Na primeira fase, o criminoso obtém informações relacionadas à identidade. Esta parte do delito, por exemplo, pode ser realizada usando softwares maliciosos ou ataques de phishing.
• A segunda fase é caracterizada pela interação com as informações de identidade antes do uso dessas informações em infrações criminais. Um exemplo é a venda de informações relacionadas à identidade. Registros de cartões de crédito são, por exemplo, vendidos por até 60 dólares americanos.
• A terceira fase é a utilização das informações relacionadas à identidade na relação com o crime. Na maioria dos casos o acesso aos dados relacionados com a identidade permite que o agressor cometa novos crimes. Os infratores estão, portanto, pouco interessados com o conjunto de dados em si, mas na capacidade de usá-los em atividades criminosas. Exemplos para esse delito pode ser a falsificação de documentos de identidade ou fraudes de cartão de crédito.

2. DIFICULDADES TÉCNICAS PARA COMBATER O CIBERCRIME

O crime virtual, assim como as tecnologias de informação, evoluem lado a lado. A partir do momento em que novas tecnologias surgem para suprir novas necessidades da sociedade moderna, as formas de cometer crimes virtuais evoluem, aproveitando-se de brechas deixadas por tais tecnologias. Desta forma, torna-se necessário que as formas de combate ao cibercrime evoluam para combater eficientemente os criminosos.

No entanto, os avanços no combate ao cibercrime não ocorrem com a mesma velocidade que estes crescem. Esse tempo perdido entre o crime a o avanço necessário para combatê-lo é o suficiente para que milhões de usuários tornem-se vítimas dos mais diversos ataques virtuais.

> The Internet is constantly undergoing development. The creation of a graphical user interface (WWW) marked the start of its dramatic expansion, as previous command-based services were less user-friendly. The creation of the WWW has enabled new applications, as well as new crimes - law enforcement agencies are struggling to keep up.[9] (GERCKE, 2009, p.74).

O crescimento exponencial do número de usuários além de aumentar o número de vítimas, torna cada vez mais complexa a investigação, uma vez que os usuários têm acesso a Internet antes de entender os seus perigos e serem devidamente educados para se prevenirem. Isso ocorre com mais frequência em países em desenvolvimento onde, apesar da popularização dos serviços de Internet, ainda contam com uma grande quantidade de usuários desinformados, mostrando-se como terreno propício ao surgimento de criminosos (*safe havens*) uma vez que tais países ainda não contém regras e leis nem recursos técnicos para regular o comportamento dos usuários no ambiente virtual. A causa é o crescimento acelerado dessas novas tecnologias em contrapartida à lenta produção legislativa e desenvolvimento técnico para coibir os abusos decorrentes do mau uso daquelas.

Os equipamentos utilizados por esses criminosos são iguais a qualquer computador pessoal, pois, na verdade, a capacidade e velocidade da máquina pouco importa e o que mais influencia é a capacidade do criminoso, ou seja, o conhecimento do criminoso acerca dos

[9] A Internet está constantemente em desenvolvimento. A criação de uma interface gráfica (WWW) marcou o início de sua expansão dramática, pois os antigos serviços baseados em comandos eram menos amigáveis. A criação da WWW permitiu novas aplicações, bem como novos crimes - as autoridades policiais estão lutando para manter-se.

processos a serem seguidos e softwares a serem usados. Pode se encontrar livremente na Internet, quando não desenvolvidos pelo próprio criminoso, diversos tipos de ferramentas tecnológicas para invasão e prática de crimes nos ambientes virtuais.

> With regards to hardware, the power of computers grows continuously. There are a number of initiatives to enable people in developing countries to use ICTs more widely. Criminals can commit serious computer crimes with only cheap or second-hand computer technology - knowledge counts for far more than equipment.[10] (GERCKE, 2009, p.66).

Visto esses dois fatores, volta-se à necessidade de uma conexão com a rede virtual. Um artifício muito usado por criminosos é o *wardriving* que consiste na busca por uma conexão wireless aberta, uma vez encontrada essa conexão, seja ela pública como a de um shopping ou privada como a de uma residência, o criminoso marca o lugar e passa a acessar a conexão sempre que necessário. Ao contrário do que se pensa, nem sempre é necessário que haja locomoção, pois é possível conectar-se a uma rede localizada até 40km de distância, com equipamentos especiais. Alguns criminosos chegam a disponibilizar a localidade de redes desse tipo na Internet. Essa prática aliada à dificuldade de rastreamento do agressor e ainda a transnacionalidade da agressão, diretamente ligados aos *safe havens* impõem grandes desafios ao combate ao cibercrime.

Outro fator a ser adicionado a essa lista é o da automação. Uma das grandes vantagens das tecnologias da informação é a de automatizar processos a fim de aumentar a velocidade e diminuir os custos. No entanto, esse artifício também é usado pelos criminosos tornando possível o controle de várias maquinas, mesmo sem que o criminoso esteja presente na rede. Aquele, aliado as chamadas *botnets*, são perfeitos para ataques de DoS (*Denial of Service*).

Velocidade é sempre importante para sistemas de informação, no entanto, pode também ser uma vulnerabilidade. À medida que as informações são trocadas rapidamente, uma vez que uma informação seja disponibilizada é praticamente impossível fazer ela desaparecer. Além disso, os registros em servidores dificilmente são mantidos por longos períodos de tempo, devido á grande quantidade de tráfego e de informação, sendo assim apagados e desaparecendo com qualquer rastro que possa ter sido deixado pelo criminoso.

[10] Com relação ao hardware, o poder dos computadores cresce continuamente. Há uma série de iniciativas que permitem que as pessoas nos países em desenvolvimento utilizem as TIC. Os criminosos podem cometer crimes graves com tecnologias de computador baratas ou de segunda mão – conhecimento conta muito mais do que equipamento.

Esse é um dos grandes problemas para investigações de cibercrime, pois devido à transnacionalidade quase sempre será necessário algum tipo de cooperação para que as informações requisitadas sejam disponibilizadas e, infelizmente, tal processo leva mais tempo do que o necessário para que elas sejam apagadas.

3. DIFICULDADES LEGAIS: TIPIFICAÇÕES INSUFICIENTES

A busca pelo criminoso não é a única dificuldade no combate ao cibercrime, mesmo que o criminoso seja identificado, ainda assim, ele pode andar em liberdade e isso se dá devido à dificuldade de acusá-lo de algum crime, pois não há lei tipificando a conduta[11]. Ainda que seja identificado e localizado, o criminoso virtual continua praticando seus delitos sem que haja a possibilidade de retaliação.

No mundo globalizado, as informações trafegam rapidamente e isso influencia a velocidade em que novas tecnologias surgem. No entanto, os processos jurídicos carecem dessa mesma dinamicidade. Logo, a velocidade em que as tecnologias evoluem é sempre maior do que os processos políticos que surgem para regulá-las.

O surgimento de novas tecnologias, ao mesmo tempo em que facilita e torna-se necessária para a sociedade internacional, também possibilita novas formas para que os crimes sejam realizados e essas evoluem mais rapidamente do que os processos jurídicos. A possibilidade de um novo tipo de agressão surgir sem que haja qualquer forma de classificá-la como crime não é algo difícil de acontecer. Esse fator já é difícil de lidar quando falamos de política doméstica, tornando-se mais complexo quando o crime virtual ocorre em escala global, o que dificulta ainda mais o processo. Logo o direito internacional, com convenções internacionais e acordos de cooperação entre os estados, torna-se arma necessária no combate aos crimes virtuais.

Em alguns casos, o mesmo direito que seria responsável por proteger os indivíduos dos criminosos também serve como escudo para estes. Muitas medidas que poderiam ser tomadas pelas autoridades, facilitando bastante a interceptação e captura dos criminosos, tornam-se inviáveis a partir do momento que iria limitar ou suprimir direitos básicos da sociedade. Uma vez que o criminoso não é identificado torna-se extremamente difícil de separá-lo e persegui-lo sem que o direito de alguns seja comprometido. O que ocorre com frequência é o balanceamento das perdas e ganhos na adoção de determinada medida.

Da mesma forma que as práticas do direito evoluem para suprir as necessidades dessa nova dinâmica existe outro fator a ser considerado no que se refere a evidências de crimes realizados. Uma vez que o delito é cometido no meio virtual as evidências do mesmo são

[11] No Brasil, o princípio da reserva legal estabelecida no art. 1º do Código Penal – "Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal".

compostas por dados virtuais. Esses dados são registros que podem ser modificados ou forjados com mais facilidade do que os documentos físicos, logo a forense computacional[12] torna-se importante aliada no que se refere à identificação desses dados e a preservação dos mesmos.

É notável a importância de especialistas na área quando nos referimos a crimes praticados no meio virtual. O direito sozinho é incapaz de fazer avanços significantes sem que haja ajuda técnica.

A Convenção sobre Cibercrime serve como guia para os países que ainda não tem legislação própria e facilita a cooperação para os que já possuem, pré-definindo fatores significantes nas negociações e melhorando a velocidade das negociações. Necessário se faz uma atualização constante dos ordenamentos internos com novas tipificações para as diversas situações de violações de direitos encontradas no ciberespaço. A Convenção do Cibercrime também prevê mecanismos de combate e principais formas de prevenir tais violações. No entanto, fatores legais não são suficientes para combates tais crimes, logo um tipo diferente de cooperação é requisitada.

[12] Ver Glossário.

4. MECANISMOS DE COMBATE AO CIBERCRIME

Com o desenvolvimento das tecnologias de informação os desafios técnicos e legais no combate ao cibercrime também sofrem mudanças, dessa forma é essencial a criação de métodos eficazes de combater ou prevenir a prática dessas ações nocivas. Essas práticas criminosas prejudicam também os países, o que evidência a necessidade de mecanismos de combate eficazes para uma maior cibersegurança.

A UIT propõe uma Agenda Global de Cibersegurança (AGC) que tem como tarefa propor um quadro para facilitar a adoção de medidas contra o crime cibernético. Para que as medidas adotadas tenham sucesso a AGC propõe cinco pilares que devem ser trabalhados para que o crime possa ser combatido de forma eficaz.

O primeiro pilar está ligado à adoção de medidas legais que visam tipificar e punir os atos dos cibercriminosos, uma vez que muitas ainda não são previstas na legislação corrente ou não têm caráter global.

O segundo pilar refere-se ao desenvolvimento de medidas técnicas de proteção que visam dificultar a pratica do crime. Essa pode se dar através dos próprios indivíduos ou empresas ou através de programas de software de segurança e provedores de Internet.

O terceiro pilar seria a instituição de estruturas organizacionais fortes e estáveis.

O quarto pilar visa a capacitação e educação de usuários, visto que a maioria dos crimes são cometidos por causa da falta de conhecimento do usuário final.

O quinto e último pilar visa a cooperação internacional, haja vista a importância para o combate ao cibercrime ser inquestionável[13] considerar a transnacionalidade do crime, é impossível o combate efetivo sem que grande parte dos países estejam em sintonia com todos os pilares anteriores.

Em função desses cinco pilares e em especial o quinto, diversas organizações internacionais buscam desenvolver formas de combater esses crimes, mas a possibilidade do crime ser realizado em qualquer território impede que os países desenvolvidos resolvam esse problema sem a participação dos países em desenvolvimento. No entanto, para que estes possam acompanhar as medidas necessárias é preciso que haja uma cooperação técnica com o intuito de desenvolver os pilares necessários em países deficitários.

[13] Podemos perceber isso pela preocupação de várias organizações em acabar com os *safe havens* e constituir uma forma global de tipificar os crimes.

4.1. Cooperação Internacional Contra o Cibercrime

Neste ponto já está claro a necessidade da unificação de um sistema de regras para combater os crimes cibernéticos. No entanto, países em desenvolvimento e desenvolvidos não têm a mesma capacidade para que regras universais possam ser instituídas, dessa forma são necessárias abordagens diferentes para cada um. O combate ao cibercrime é interesse de ambos os países e para que isto seja solucionado é necessária uma ajuda mútua. A partir do momento que os países desenvolvidos ajudam os países em desenvolvimento por meios de cooperações, esses desenvolvem instituições e técnicas necessárias ao combate do cibercrime, facilitando a adoção de políticas e extinguindo *safe havens*. Dessa forma os países em desenvolvimento perdem menos com esse tipo de crime e os em desenvolvimento ganha mais capacidade tecnológica de combatê-los. A cooperação é indispensável para combater o cibercrime e os ganhos são mútuos.

Segundo os princípios da cooperação técnica trabalhados por Filho (2007) a cooperação técnica baseia-se nos interesses mútuos e traz o a tona os sentidos de equidade e ética, para fins de desenvolvimento. Desenvolvimento esse que não para no país receptor, ele se espalha, garantindo um maior desenvolvimento dos países como um grupo e ocasionando iniciativas multilaterais viáveis para diminuição de gastos da cooperação.

Outro fator que pode emergir como ajuda para solução do problema é a cooperação entre países em desenvolvimento, o que proporciona uma maior sincronia em termos de políticas. No entanto, a cooperação com finalidade de desenvolver a fim de igualar as potencialidades não é a única preocupação. Também é necessária a instituição de regras universais de combate ao cibercrime. Devido a importância de um dos pilares citados anteriormente, no que se refere a construção de estruturas organizacionais, as organizações internacionais são a forma mais forte de combater tais crimes, pois consistem na forma mais institucionalizada de cooperação internacional (HERZ; HOFFMANN, 2004). Veremos o que algumas delas têm a dizer sobre o combate ao cibercrime.

4.1.1. Internet Governance Forum

Com a finalidade de apoiar o Secretariado-Geral, na realização do mandato da Cúpula Mundial da Sociedade da Informação (World Summit on the Information Society-WSIS)

houve a convocação de um novo fórum para o diálogo político multi-interesse (multi-stakeholder) - o Internet Governance Forum (IGF).

O IGF foi criado e instituído a partir da Agenda Túnis para a Sociedade da Informação, uma declaração de consenso da Cúpula Mundial sobre a Sociedade da Informação, aprovado em 18 de novembro de 2005 em Tunis, Tunísia. O principal propósito do IGF é proporcionar um espaço para discussão sobre a governança na Internet, proporcionando uma abertura para intelectuais e empresas expor suas idéias sobre o tema. O Brasil faz parte do IGF e sediou uma de suas reuniões em 2007.

O parágrafo 72 da agenda Tunis traz todas as tarefas do IGF :

> **72.**Pedimos ao secretário-geral da ONU, em um processo aberto e inclusivo, para convocar, até o segundo trimestre de 2006, uma reunião do novo fórum para o diálogo político multi-stakeholder chamado o Internet Governance Forum (IGF). O mandato do fórum é:
>
> 1. Discutir questões de políticas públicas relacionadas com os elementos-chave da governança da Internet a fim de promover a sustentabilidade, robustez, segurança, estabilidade e desenvolvimento da Internet;
> 2. Facilitar o discurso entre os organismos que tratam diferentes políticas públicas relativas à Internet e discutir questões que não se enquadram no âmbito de qualquer órgão existente;
> 3. Relacionar-se com diferentes organizações inter-governamentais e outras instituições sobre assuntos da sua competência;
> 4. Facilitar a troca de informações e melhores práticas, e neste contexto fazer pleno uso dos conhecimentos das comunidades acadêmica, científica e técnica;
> 5. Assessorar todos os interessados em propor formas e meios de acelerar a disponibilidade e acessibilidade da Internet no mundo em desenvolvimento;
> 6. Fortalecer e melhorar o engajamento das partes interessadas no registro e / ou mecanismos de governança da Internet futuro, particularmente aquelas de países em desenvolvimento;
> 7. Identificar temas emergentes, trazê-los à atenção dos órgãos competentes e ao público em geral, e, se necessário, fazer recomendações;
> 8. Contribuir para a capacitação para a governança da Internet nos países em desenvolvimento, desenho totalmente em fontes locais de conhecimento e especialização;
> 9. Promover e avaliar, numa base contínua, a incorporação dos princípios da WSIS em processos de governança da Internet;
> 10. Discutir, as questões relativas aos recursos críticos da Internet;
> 11. Ajuda para encontrar soluções para os problemas decorrentes do uso e abuso da Internet, de particular interesse para utilizadores diários. (INTERNATIONAL TELECOMMUNICATION UNION, 2005, tradução nossa)

A tentativa de prover um diálogo entre as políticas e proporcionar idéias sobre novas políticas, é uma forma de ajudar os países ainda em desenvolvimento a promoverem possíveis leis sobre as ações de seus cidadãos na Internet. O IGF é uma organização mais preocupada com a informação do que com a implementação de políticas, há certo reconhecimento de que

nos países em desenvolvimento a implementação de tais políticas não podem seguir os mesmo parâmetros de países mais desenvolvidos, onde as políticas são mais complexas e a governança na internet é uma realidade mais visível.

Favorecer, melhorar e disponibilizar os recursos relativos a Internet em países em desenvolvimento é ação primordial para o desenvolvimento de políticas de governança, uma vez que é necessário um maior conhecimento e preparação técnica para que tais políticas tenham efeito. Essas técnicas não são inerentes a países em desenvolvimento, uma vez que se adquiriu tecnologia numa estrutura totalmente diferente.

No entanto, torna-se necessário uma assistência aos países subdesenvolvidos, não apenas no que se refere a diferenciá-los em termos de criação de política, mas ampará-los com modelos ou alternativas para adoção de políticas. O cibercrime é uma preocupação mundial e que ultrapassa fronteiras, sendo necessário uma maior unificação ou ainda uma maior harmonia entre as leis dos países, esforços individuais dificilmente seriam significantes. Nesse sentido, a cooperação internacional torna-se arma primordial no combate. Veremos os meios de cooperação mais significantes a seguir.

4.1.2. G8

Em 1997, o G8 estabeleceu um subgrupo para lidar com crimes tecnológicos. No início, esse subgrupo tinha o papel de investigar crimes cibernéticos e com o tempo foi evoluindo de forma a ajudar países subdesenvolvidos a desenvolver-se no combate a esses crimes. A participação de países em desenvolvimento dava-se, principalmente, pelo fato do G8 querer prevenir o surgimento de *safe havens (GERCKE, 2009, p.89)*, o maior interesse da organização em fazer com que os países desenvolvidos participem esta associado a esse objetivo.

Um dos maiores avanços do G8 é a criação de uma rede de informações que interliga os países e está disponível 24 horas por dia, 7 dias por semana. A rede é de extrema importância para o combate ao cibercrime, uma vez que agiliza a troca de informações e possibilita uma maior articulação das autoridades que disponibilizam desse sistema. Esse tipo

de sistema também é usado por várias organizações internacionais para o combate de crimes entre fronteiras[14].

4.1.3. ONU

Em 1994 a ONU criou um manual para prevenção de crimes relacionados a computadores, baseada na resolução 45/121 o manual serve como um guia, similar ao publicado pela UIT, e serve mais como uma fonte de pesquisa do que um documento regulador. Somente em 2000, que a Assembléia Geral adotou uma resolução para combater o uso criminoso das TIC. A resolução indica algumas medidas necessárias ao combate ao cibercrime e mostra interesses similares aos do G8.

> (A) Os Estados devem assegurar que suas leis e práticas eliminam safe havens para aqueles fazem mal uso das tecnologias da informação;
> (B) A cooperação na aplicação da lei na investigação e repressão de casos internacionais de uso criminoso das tecnologias da informação deve ser coordenado entre todos os Estados interessados;
> (C) Devem ser trocadas informações entre os Estados sobre os problemas que eles enfrentam na luta contra o uso criminoso das tecnologias da informação;
> (D) Os aplicadores da lei devem ser treinados e equipados para lidar com o uso criminoso das tecnologias da informação;
> (E) Os sistemas jurídicos devem proteger a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos de uma imparidade não autorizada e garantir que o abuso é penalizado;
> (F) Os sistemas jurídicos devem permitir a preservação e o acesso rápido aos dados eletrônicos relativos a investigações criminais;
> (G) Regimes de assistência mútua deve assegurar uma rápida investigação do uso criminoso das tecnologias da informação e troca de provas;
> (H) O público em geral deve estar cientes da necessidade de prevenir e combater o uso criminoso das tecnologias da informação;
> (I) Na medida do possível, tecnologias de informação devem ser projetadas para ajudar a prevenir e detectar o uso criminoso, rastrear criminosos e reunir provas;
> (J) A luta contra o uso criminoso das tecnologias da informação requer o desenvolvimento de soluções tendo em conta tanto a proteção das liberdades individuais e da privacidade quanto a preservação da capacidade dos governos para combater a má utilização criminosa; (UNITED NATIONS, 2001, tradução nossa)

Prevenir a existência de *safe haven*s é, mais uma vez, uma prioridade. É possível notar que muitas dessas medidas se tornam inviáveis e muito custosas para países em desenvolvimento o que também reforça a necessidade de uma cooperação. A UNCTAD

[14] Tanto a Interpol quanto a Convenção sobre Cibercrime usam esse sistema, mas não é claro se o sistema é o mesmo ou se foi criado um para cada organização.

estabeleceu algumas importâncias no que se refere a combater crimes virtuais visando os países em desenvolvimento e reconhece sua importância para combater os crimes virtuais.

> Cybercrime is often international in nature, occurring across boundaries and impacting on users in different countries. Developing countries will obviously be both victims and the source of cybercrime. As noted at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, in April 2005, developing countries "have become staging grounds for attacks by cyber criminals" on developed countries, due to the greater prevalence of unprotected systems. To address this interrelated vulnerability, greater harmonization evolves between jurisdictions in order to be able to effectively prevent criminal activities, as well as pursue perpetrators. In recent years, there have been a number of initiatives at the intergovernmental level, including the United Nations, the Council of Europe, the G8 and the Commonwealth. These will be used as a benchmark to consider the needs of developing countries.[15] (UNCTAD, 2005)

Apesar dos países em desenvolvimento não poderem participar efetivamente na Convenção sobre Cibercrime, essa serve como um tipo de medida para as necessidades que terão esses países para o desenvolvimento de políticas anti-cibercrime. Além disso, a ONU está comprometida a fazer com que os países desenvolvidos intensifiquem o apoio dado aos países em desenvolvimento para construir recursos para combater o cibercrime e harmonizar a legislação nacional (BALLARD, 2010).

4.1.4. Convenção Sobre Cibercrime

Com 47 países signatários, sendo 4 desses fora da Europa (Japão, Estados Unidos, Canadá e África do Sul), a Convenção Sobre Cibercrime entrou em vigor em julho de 2004 e é o único tratado internacional sobre o assunto. Estabelecendo diretrizes para todos os governos que pretendam desenvolver a legislação contra o cibercrime, a convenção é aberta a assinatura por parte de países não europeus prevendo um quadro para a cooperação internacional nestes domínios.

---

[15] Cibercrime é muitas vezes de natureza internacional, ocorrendo através das fronteiras e têm impacto sobre os usuários em diferentes países. Os países em desenvolvimento serão, obviamente, as vítimas e fonte de crimes cibernéticos. Como observado no XI Congresso das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal, em abril de 2005, os países em desenvolvimento "se tornaram pontos de apoio para ataques de criminosos virtuais" nos países desenvolvidos, devido à maior prevalência de sistemas desprotegidos. Para lidar com essa vulnerabilidade inter-relacionada, uma maior harmonização evolui entre as jurisdições de modo a ser capaz de efetivamente impedir atividades criminosas, bem como perseguir perpretadores. Nos últimos anos, tem havido uma série de iniciativas ao nível intergovernamental, incluindo as Nações Unidas, o Conselho Europeu, o G8 e a Commonwealth. Estes serão utilizados como referência para considerar as necessidades dos países em desenvolvimento.

A Convenção é o primeiro tratado internacional sobre crimes cometidos através da Internet e outras redes informáticas, os principais crimes combatidos por ela são: acesso ilegal a dados, a interceptação ilegal de dados, a interferência de dados, o mau uso de dispositivos de computador relacionados com a falsificação, fraude, crimes relacionados à pornografia infantil e crimes contra os direitos de autor.

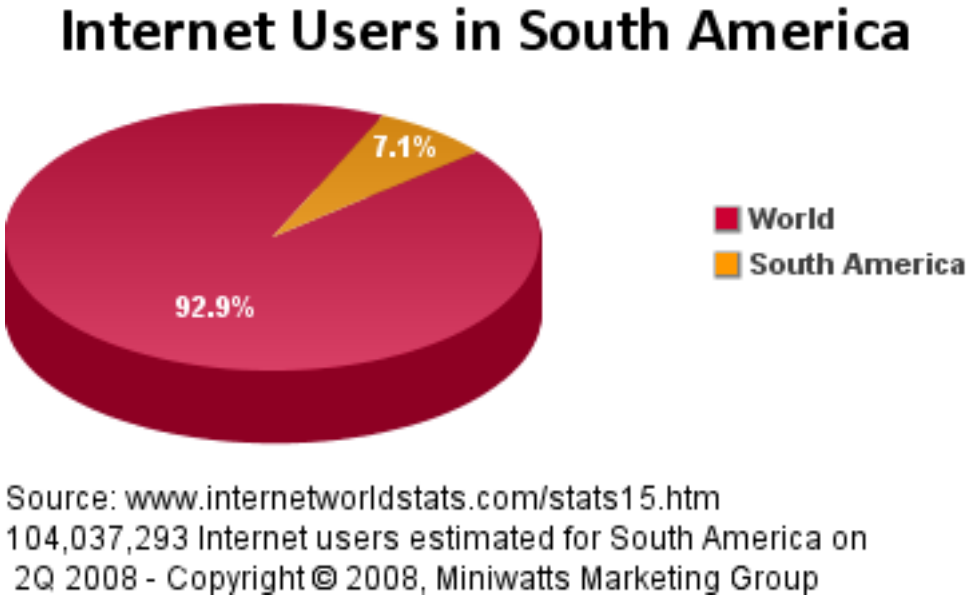
Visto que esses crimes são cometidos de forma muito líquida na rede, espalhando-se de um Estado para outro com grande velocidade, há a necessidade de instituir uma política penal comum para que os criminosos possam ser punidos, essa política pode somente ser admitida através da cooperação entre os Estados, no entanto, os Estados signatários dessa convenção têm certo grau de desenvolvimento, o que facilita a cooperação, mas não resolve o problema. Outra finalidade da criação de uma lei comum é para que os processos possam acompanhar a velocidade no qual essas relações acontecem e puni-las onde quer que o infrator esteja.

A Convenção de Budapeste, como também é chamada, é um tratado funcional que tipifica os crimes virtuais e institui parâmetros para a cooperação no combate aos mesmos. Apesar de aceitar signatários de fora do conselho, é possível notar que o tratado só serve para países com grau de desenvolvimento mais elevado. Ainda que países subdesenvolvidos não possam participar eficientemente a convenção serve como um guia para criação de políticas eficientes.

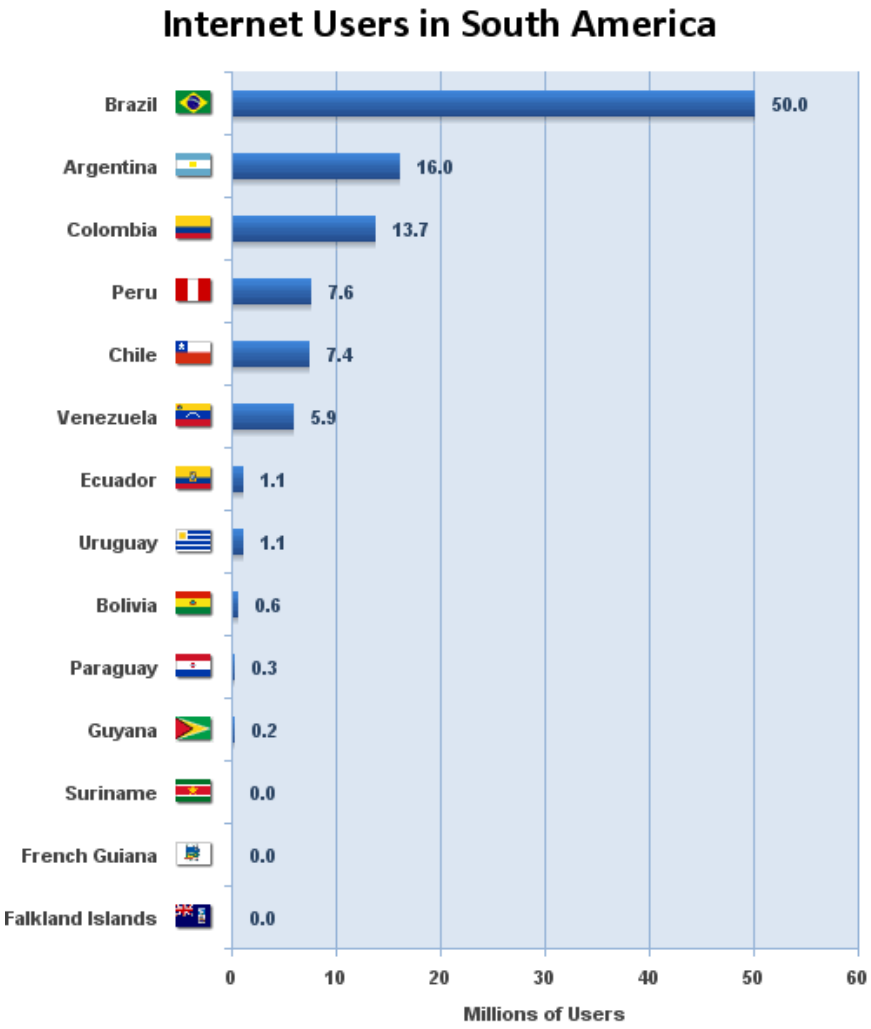
5. BRASIL: UMA VISÂO DOS PAÍSES EM DESENVOLVIMENTO

Devido ao seu maior desenvolvimento tecnológico os países desenvolvidos são mais avançados na adoção de mecanismos, no entanto devido à natureza transnacional do crime pouco pode ser feito individualmente e torna-se inviável combater o cibercrime quando o numero de "safe havens" ultrapassa o numero de países capazes de adotar políticas eficazes. A implementação de políticas nos países subdesenvolvidos não é tão fácil, as diferenças estruturais possibilitam que países desenvolvidos adotem políticas de prevenção com mais facilidade. A compatibilidade legal não é a única preocupação nesses países, é preciso analisar ainda o apoio da população e do setor privado à adoção dessas políticas. As leis sobre cibercrime no Brasil ainda estão em discussão.

Ainda é inviável para o país assinar a Convenção sobre Cibercrime[16]. A América do Sul possui apenas 7.1% dos usuários de Internet do mundo e o Brasil é o país com o maior numero de usuários de Internet. No entanto, devido a falta de capacidade de punir criminosos, o país também ocupa os 10 primeiras posições de hackers mais ativos do mundo, causando bilhões em prejuízo para os países do G8 (ÂNGELO, 2010). Os gráficos a seguir mostram dados relevantes a quantidade de usuários na America do Sul e no Brasil.



[16] BRASIL não pode aderir a convenção de Budapeste sobre o cibercrime. , 2007. Disponível em: <http:// http://www.inforel.org/noticias/noticia.php?not_id=2358&tipo=1>. Acesso em: 13 out. 2010.



Source: www.internetworldstats.com/stats15.htm
104,037,293 Internet users in South America estimated for 2Q 2008
Copyright © 2008, Miniwatts Marketing Group

No Brasil foi criado o DSIC (Departamento de Segurança da Informação e Comunicações) da Presidência da Republica com o objetivo de divulgar um conjunto de normas de segurança a serem adotadas pelos órgãos da administração pública do governo. Segundo o Artigo 8º do Decreto Nº 6.931, de 11 de agosto de 2009, os objetivos do DSIC para criação de uma política de segurança mais eficaz são:

1. Adotar as medidas necessárias e coordenar a implantação e o funcionamento do Sistema de Segurança e Credenciamento - SISC, de pessoas e empresas, no trato de assuntos, documentos e tecnologia sigilosos;
2. Planejar e coordenar a execução das atividades de segurança da informação e comunicações na administração pública federal;
3. Definir requisitos metodológicos para implementação da segurança da informação e comunicações pelos órgãos e entidades da administração pública federal;

4. Operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal;
5. Estudar legislações correlatas e implementar as propostas sobre matérias relacionadas à segurança da informação e comunicações; e
6. Avaliar tratados, acordos ou atos internacionais relacionados à segurança da informação e comunicações.

Interessante observar que um dos objetivos do DSIC para uma maior política de segurança é avaliar acordos de cooperação entre os países. No entanto, as medidas focam apenas na proteção de órgãos do governo e não ao usuário normal.

5.1. Conhecimento como Prevenção

Uma vez que o criminoso consegue as informações desejadas é praticamente impossível pará-lo, a forma mais fácil de combater esse tipo de crime é através da prevenção, para as grandes empresas e sistemas de informação de países são desenvolvidos grandes softwares de proteção, já para usuários normais são disponibilizados programas amplamente conhecidos, o fato de já serem conhecidos proporciona uma vantagem ao criminoso.

Logo a melhor forma de proteger-se é através do conhecimento. O Brasil está bem defasado quando se trata de possibilitar instrução aos usuários comuns, no entanto, esforços e resultados têm sido alcançados a partir da contribuição de uma ONG chamada de Safernet.

A Safernet trabalha em parceria com o governo federal na instrução dos usuários da internet em todo o país. Ela também trabalha com um sistema de denuncias, é uma entidade voltada para maior segurança no meio virtual através da educação dos usuários[17]. A importância da educação do usuário já foi discutida anteriormente, mas no caso de países em desenvolvimento a necessidade dessa medida é maior. Nesses países há maior incidência de *spams*, esse tipo de ataque virtual visa o usuário desinformado e causa mais danos em países em desenvolvimento do que nos desenvolvidos (GERCKE, 2009). Dessa forma a Safernet torna-se pedra angular para estabelecer um pé de igualdade quanto às perdas econômicas do país com crimes virtuais.

5.2. A Paraíba Como Pólo Anti-cibercrime

[17] Sobre a Safernet, visitar: http://www.safernet.org.br

Atualmente, a Paraíba recebeu visitas de autoridades da Associação de luta contra o cibercrime que mostraram interesse em implantar na Paraíba um pólo para combater crimes virtuais. A proposta foi apresentada no I Seminário Cibercrime e Cooperação Penal Internacional - ISCCRIM em 2009 pelo professor Mohamed Chawki[18]. A intenção a fazer da Paraíba uma referencia no combate ao cibercrime na America latina.

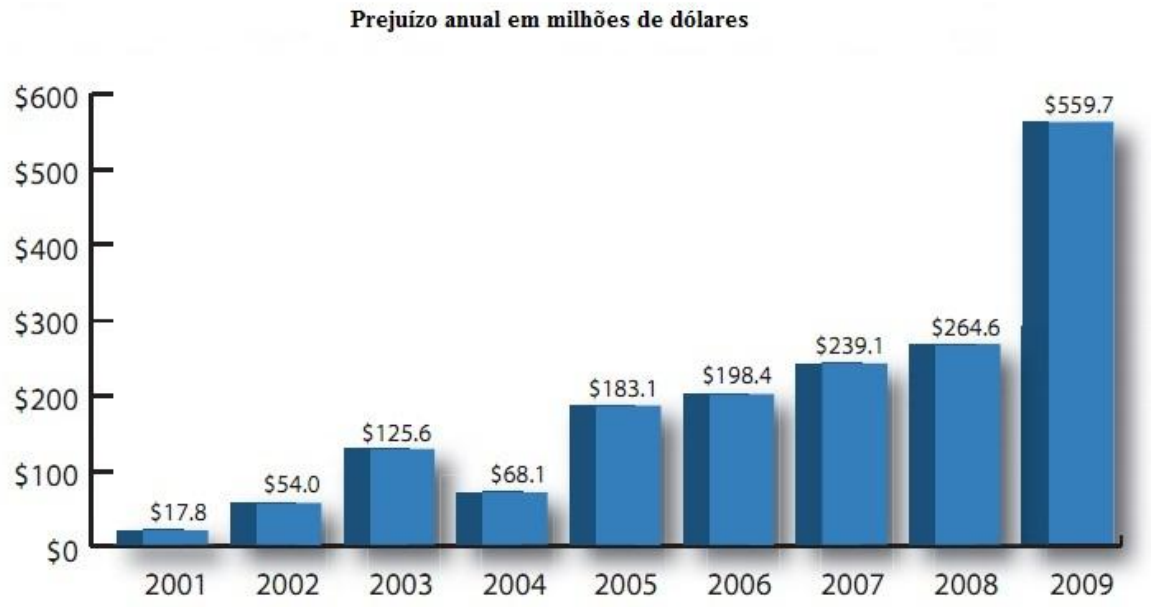
O evento teve apoio da Unipê, policia Militar e outras instituições do estado, além do Sebrae que serviria como apoio tecnológico para as propostas apresentadas. Essas instituições reconhecem o papel da cooperação internacional no combate aos crimes virtuais e acreditam que a Paraíba um papel importante na cooperação.

[18] PARAÍBA pode ganhar pólo de combate a cibercrimes. , 2009. Disponível em: <http://www.paraiba1.com.br/Noticia/24136_paraiba-pode-ganhar-polo-de-combate-a-cibercrimes.html>. Acesso em: 05 nov. 2010.

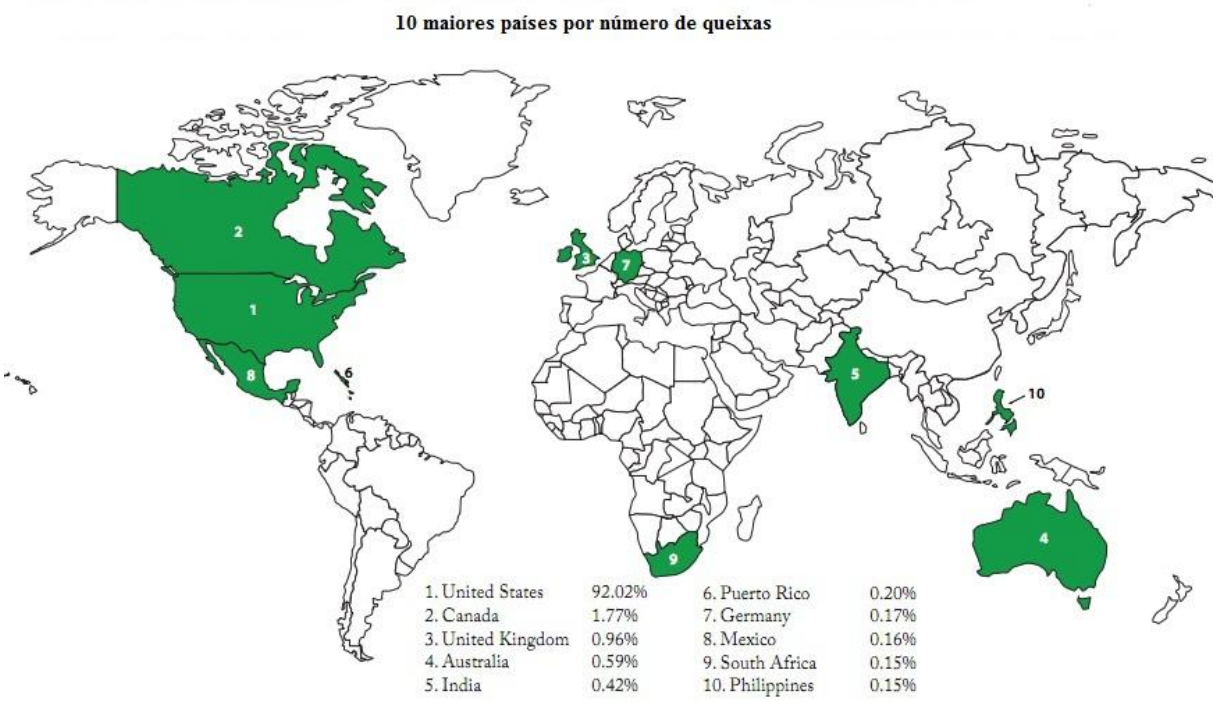
6. UMA ANÁLISE DOS CASOS ESTADOUNIDENSES

Os Estados Unidos é o país mais avançado em termos de combate aos crimes virtuais, os casos são reportados a uma instituição a Internet Crime Complaint Center (IC3) que passa o caso para ser investigado pelo FBI. A IC3 recebe cerca de 200 mil denúncias por ano, só em 2009 foram mais de 300 mil. A instituição disponibiliza relatórios anuais com estatísticas dos casos recebidos.

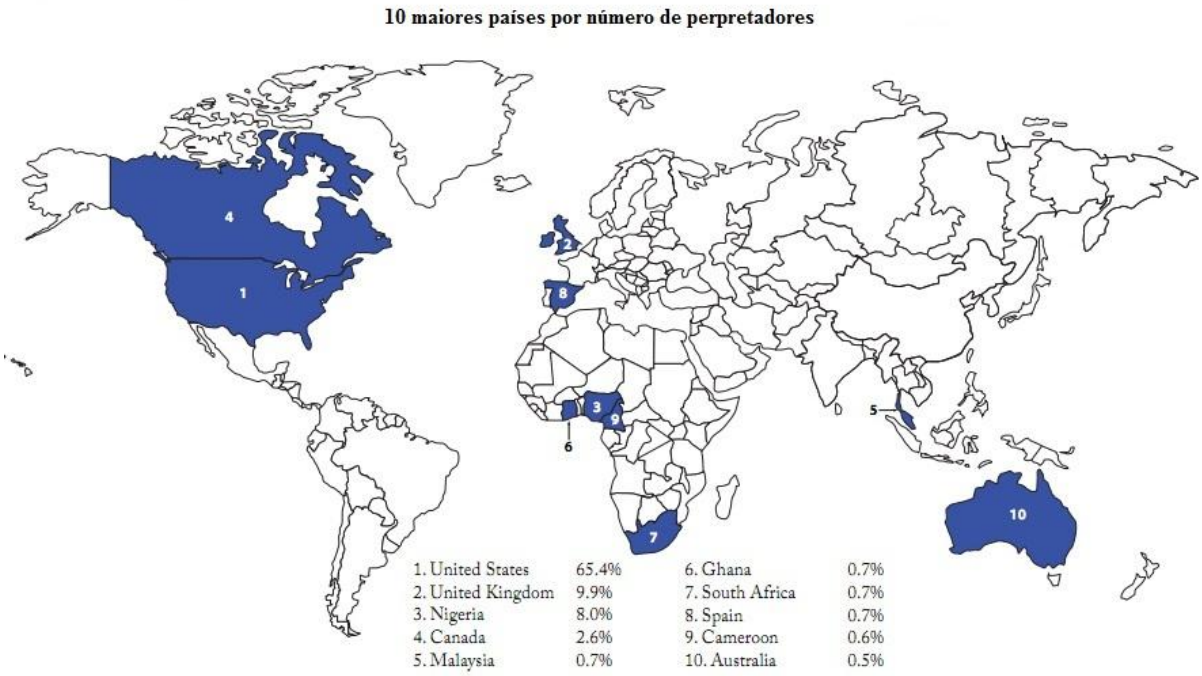
Esses são somente as denúncias recebidas pela instituição, muitos dos crimes nunca chegam a ser registrados. Esses dados são apenas para os Estados Unidos e contam com pouca participação de fora, mas ainda assim ocasiona milhões em perdas. É estimado que o cibercrime cause cerca de 1 trilhão em prejuízos por ano (WEBER, 2009).



Apesar de ser um órgão interno a IC3 também disponibiliza estatísticas sobre denúncias recebidas de fora do país, assim como país de origem dos infratores. Dificilmente isso servira para muita analise, mas mostra a importância da cooperação, visto que sem ela infratores de fora dificilmente receberão algum tipo de punição.



Abaixo se encontram os quadros de invasores:



A disparidade entre as denúncias e a localização dos infratores pode evidenciar a preferências dos mesmos por atingir alvos de outros países, visando dificultar as investigações. Mais de 90% das denúncias são feitas nos Estados Unidos, mas apenas 65,4% dos infratores estão presentes nesse território.

CONSIDERAÇÕES FINAIS

A necessidade da cooperação no combate ao Cibercrime é algo inquestionável. Quando tratamos de disparidades tecnológicas e financeiras torna-se difícil agrupar países desenvolvidos e em desenvolvimento num mesmo tratado de cooperação. Suas finalidades e habilidades para tratar o assunto são totalmente diferentes. As dinâmicas das relações entre os Estados para criação de leis contra o cibercrime são agravadas a partir do momento em que um Estado se encontra menos capaz, tecnologicamente ou economicamente, para aplicação de tais políticas. Apesar disso a falta de tecnologia ou o baixo acesso a Internet não traduz em uma maior proteção, uma vez que as ofensas podem ser cometidas por todo o planeta os países em desenvolvimento tornam-se, não apenas os causadores dos crimes, mas também as principais vítimas. Esses crimes por sua vez inibem o crescimento do país e dificultam ainda mais a adoção de políticas eficazes. Proporcionando assim um território perfeito para o surgimento de redes de criminosos que realizarão crimes em vários países.

A abertura para um diálogo sobre as possíveis soluções para problemática só tendem a aumentar e a importância dos países desenvolvidos para o combate ao cibercrime é visível, sendo assim, as instituições estabelecem guias e metas pelos quais os países possam desenvolver políticas mais efetivas. Esse diálogo político faz com que os países em desenvolvimento possam incorporar políticas já adotadas de forma compatível com suas exigências internas ocasionando maior compatibilidade legal. A ajuda dos países desenvolvidos no que se refere a estabelecer estratégias faz com que os países em desenvolvimento possam adotar políticas com custo e tempo reduzido.

> One possibility is that anti-cybercrime strategies developed in industrialized countries could be introduced in developing countries, offering advantages of reduced cost and time for development. The implementation of existing strategies could enable developing countries to benefit from existing insights and experience.[19] (GERCKE, 2009, p.84).

Desta forma os principais tratados, reconhecendo a importância da eliminação de *safe havens,* passando a preocupar-se com a participação dos países subdesenvolvidos. A

[19] Uma possibilidade é que as estratégias anti-cibercrime desenvolvidas nos países industrializados poderiam ser introduzidas em países em desenvolvimento, oferecendo vantagens de custo reduzido e tempo de desenvolvimento. A implementação de estratégias existentes poderia permitir aos países em desenvolvimento a beneficiar de conhecimentos e experiências existentes.

preferência pelo ataque a outros países é clara e as dificuldades técnicas e legais impossibilitam a resolução dos crimes ocorridos entre fronteiras sem que haja qualquer tipo de cooperação. O Brasil, apesar de não ter leis fortes no combate a crimes virtuais já se apresenta como interesse de outros países, além de receber iniciativas privadas para ajudar na solução do problema. A educação dos usuários da internet está acontecendo de forma mais lenta do que a velocidade com que a internet se espalha no país, mas os esforços da Safernet mostram, não apenas o poder da iniciativa privada, mas como é possível adquirir maior poder de barganha frente às negociações, uma vez que minimizando as perdas com cibercrime o Brasil pode igualar-se, em termos de interesse, aos países mais desenvolvidos.

REFERÊNCIAS

ÂNGELO, Fernanda. **Brasil lidera ranking mundial de hackers e crimes virtuais.** , 2002. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u11609.shtml>. Acesso em: 07 ago. 2010.

BALLARD, Mark. **Un rejects international cybercrime treaty.** , 2010. Disponível em: <http://www.computerweekly.com/Articles/2010/04/20/240973/UN-rejects-international-cybercrime-treaty.htm>. Acesso em: 05 nov. 2010.

CASTELLS, Manuel. **A sociedade em rede.** São Paulo: Paz E Terra, 2007.

COUNCIL OF EUROPE. **Convention on cybercrime.** , 2001. Disponível em: <http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>. Acesso em: 07 ago. 2010.

DANTAS, Agnes. **Internet mais segura depende de cooperação internacional, defendem especialistas.** , 2007. Disponível em: <http://oglobo.globo.com/tecnologia/mat/2007/11/14/327171371.asp>. Acesso em: 07 ago. 2010.

FILHO, Wladimir Valler. **Aspectos da cooperação técnica internacional.** In: O brasil e a crise haitiana. Brasília: Thesaurus, 2007. p.25-57.

GAREY, Lorna. **Cybercrime as an economic threat.** , 2010. Disponível em: <http://www.informationweek.com/blog/main/archives/2010/02/cybercrime_as_a.html>. Acesso em: 07 ago. 2010.

GERCKE, Marco. **Understanding cybercrime: a guide for developing countries.** , 2009. Disponível em: <http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html>. Acesso em: 07 ago. 2010.

HERZ, Mônica; HOFFMANN, Andrea Ribeiro. **Organizações internacionais: História e práticas.** Rio de Janeiro: Elsevier, 2004.

INTERNATIONAL TELECOMMUNICATION UNION. **Tunis agenda for the information society.** , 2005. Disponível em: <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>. Acesso em: 07 ago. 2010.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal.** São Paulo: Memória Jurídica, 2004.

TOFFLER, Alvin; TOFFLER, Heidi. **A riqueza revolucionária.** São Paulo: Futura, 2007.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. **Information economy report 2005.** , 2005. Disponível em: <http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf>. Acesso em: 10 set. 2010.

UNITED NATIONS. **Resolution adopted by the general assembly: [on the report of the Third Committee (A/55/593)].** , 2001. Disponível em: <http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf>. Acesso em: 07 ago. 2010.

UNITED NATIONS. **United nations manual on the prevention and control of computer-related crime.** , 1994. Disponível em: <http://www.uncjin.org/Documents/EighthCongress.html>. Acesso em: 07 ago. 2010.

WEBER, Tim. **Cybercrime threat rising sharply.** , 2009. Disponível em: <http://news.bbc.co.uk/2/hi/business/davos/7862549.stm>. Acesso em: 07 ago. 2010.

GLOSSÁRIO

AGC: Agenda Global de Cibersegurança é um quadro proposto pela UIT com medidas a serem tomadas ao adotar políticas contra o cibercrime para que essas sejam eficazes.

Botnets: redes de computadores infectados e conectados na internet que podem ser controlados remotamente pelo agressor ou ainda automatizados para fazer a mesma ação varias vezes.

DoS: sigla que significa “Denial of Service”, um tipo de ataque virtual a servidores efetuados por hackers, muito efetivo para derrubada de determinado serviço, é efetuado geralmente a partir da solicitação de milhões de conexões ao mesmo tempo efetuadas por botnets.

Forense computacional: métodos de investigação criminalística que consiste na aquisição, preservação e restauração de evidencias de crimes virtuais.

Napster: programa de compartilhamento de arquivos.

Phishing: utilização de e-mails como forma de obter dados sobre a vítima.

Provedor de acesso: disponibiliza serviços de acesso a internet, e-mail, hospedagem de sites, entre outros.

Servidor: um sistema de computadores que fornece um serviço a uma rede de computadores.

Spam: envio de mensagens em massa.

TIC: Tecnologias da informação e comunicação, são todas tecnologias usadas a fim de transferir ou adquirir informações.

VoIP: Transmissão de Voz sobre IP, isto é, usar a rede de Internet para transmissão de telefonia.