Um Estudo da Necessidade de Informação como Estratégia para Combate ao Crime Cibernético

Felipe Lopes da Cruz
Jorge Henrique C Fernandes

RESUMO

A necessidade de adoção de medidas voltadas à intimidação aos delituosos pelo crime cibernético se justifica pelas previsões que indicam seu crescimento e impacto negativo para a sociedade da informação. Entre outros fatores, o crescimento do Crime Cibernético é em parte decorrente da falta de legislação específica que tipifique os crimes, bem como das vulnerabilidades apresentadas pelos sistemas de segurança. Este artigo apresenta resultados preliminares da aplicação de um estudo da necessidade de informação dos atores envolvidos no processo interativo via internet: usuários, empresas, criminosos e organizações de combate ao crime cibernético. Trata-se de uma estratégia para a antecipação, a prevenção e o combate.

Palavras-chave: Informação. Estratégia. Crime Cibernético.

Introdução

A busca pela maximização do lucro por meio da concepção de estratégias de atuação que dificultem o rastreamento das atividades ilícitas e, como conseqüência, a punição dos envolvidos, são características presentes nas organizações criminosas.

O advento da internet, a ocupação do ciberespaço por relações entre cliente e empresas baseadas na movimentação de valores e a popularização do acesso online a produtos e serviços transformaram este canal de comunicação digital em ambiente propício à consecução de crimes.

Recebido em 31 de março de 2009.
Aceito em 1 de agosto de 2009.

Além destes, outros fatores contribuem para o avanço da criminalidade neste meio por dificultarem a ação das instituições responsáveis pela prevenção e repressão das atitudes ilícitas, entre eles: a interação independente da identificação formal do usuário; a possibilidade da troca de informações em tempo real; a internacionalidade do acesso; e o avanço constante da tecnologia que não consegue ser apreendido na sua plenitude pelos usuários.

> *Cumpre lembrar que, a existência de um mundo virtual ou ciberespaço, que apresenta novas concepções de tempo e espaço, bem como as dificuldades de identificação dos usuários da Internet, além dos entraves que surgem no campo da produção de provas, dentre outros aspectos, constituem verdadeiros óbices no combate à criminalidade informática (Santos, 2008).*

Para transpor os obstáculos que dificultam a repressão no meio digital e acabam incentivando a migração das organizações criminosas para este espaço, faz-se necessário levantar os elementos integrantes do processo de interação no meio. Este processo descreve a relação de cada elemento (usuários, criminosos e sistemas computacionais) com o fluxo de informações que viabilizam o crime. Com isso é possível propor estratégias que permitam a sua prevenção e punição.

A proximidade e a troca de informações entre as empresas e os usuários – vítimas dos crimes cibernéticos – e as instituições de segurança é essencial para proporcionar o entendimento do modus operandi dos agentes dos crimes. Isto levará à criação de táticas específicas para a repressão uniforme e abrangente dos delitos.

Este artigo descreve a importância dos estudos de necessidades de informação como estratégicos para o desenvolvimento de planos específicos, inclusive de sistemas de informação, voltados à repressão aos crimes cibernéticos. Tais estudos têm com base o entendimento das demandas por informação (informacionais) das entidades envolvidas no processo interativo via internet – usuários, empresas, criminosos e instituições de combate ao crime em ambiente virtual.

Crimes Cibernéticos

Legislações sobre crimes cibernéticos encontram-se na pauta de discussões e votações do congresso nacional (Senado, 2008). Sejam aprovadas ou não, alguma forma de regulação para os crimes cibernéticos se faz necessária, que seja pelos menos a discussão e compreensão dos mecanismos que se encontram por trás dos crimes cibernéticos e suas formas de repressão por diversos mecanismos do Estado.

TÍTULO	TEMA
1	Crimes contra a confidencialidade, integridade e disponibilidade de dados de computador e sistemas.
2	Crimes através de computadores [fraude e falsificação].
3	Crimes relacionados ao conteúdo [pornografia infantil].
4	Crimes relacionados à infração da propriedade intelectual e direitos conexos.
5	Responsabilidade subsidiária e sanções [esforço e auxílio ou responsabilização corporativa].

Tabela 1. Tipificação de Crimes Cibernéticos no Tratado de Budapeste.

Segundo Perrin (2006), o termo "cibercrime" foi cunhado no final da década de 90, em encontro voltado ao estudo dos problemas da criminalidade relacionados à internet, do qual participou um grupo de nações integrantes do G8, e foi utilizado para tipificar os crimes perpetrados na internet ou nas novas redes de telecomunicações. A autora afirma que, por intervenção deste grupo, o Conselho Europeu criou a Convenção sobre o Cibercrime (COE, 2001), também chamada de Tratado de Budapeste, onde são descritas diversas recomendações e áreas sujeitas a mudanças na legislação de países, dentre as quais se destacam as indicadas na Tabela 1.

Cabe ressaltar que as condutas relacionadas aos crimes praticados em ambiente virtual nem sempre caracterizam novos crimes. Em muitos casos, o ambiente virtual é apenas o meio utilizado para a realização das atitudes ilícitas.

[...] o crime virtual é qualquer ação típica, antijurídica e culpável cometida contra

> *ou pela utilização de processamento automático de dados ou sua transmissão em que um computador conectado à rede mundial de computadores – Internet – seja o instrumento ou o objeto do delito. (Pinheiro, 2006).*

Segundo Pinheiro (2006), existem autores que classificam os crimes cibernéticos em puros e impuros (ou mistos), sendo puros os crimes não tipificados por leis que especifiquem as condutas; e os impuros ou mistos, que são tipos penais previstos no Código Penal e que podem também ocorrer no ciberespaço. A autora propõe, ainda, uma lista de crimes que podem ser realizados por meio da internet, sendo eles:

- Crimes contra a honra: calúnia, difamação e injúria;
- Crimes contra a liberdade individual: ameaça, inviolabilidade de correspondência, divulgação de segredos, divulgação de segredos contidos ou não em sistemas de informação ou bancos de dados da Administração Pública;
- Crimes contra o patrimônio: furto, extorsão, dano e estelionato;
- Crimes contra os costumes: favorecimento à prostituição, de escrito ou objeto obsceno e pedofilia;
- Outros crimes: lavagem de dinheiro e invasões de privacidade; pixações em sítios oficiais do governo; vandalismo; sabotagem; crimes contra a paz pública; pirataria em geral; espionagem; lesões a direitos humanos (terrorismo, crimes de ódio, racismo, etc); destruição de informações; jogos ilegais; falsificação do selo ou sinal público; falsidade ideológica; modificação ou alteração não autorizada de sistema de informação; violação de sigilo funcional; e fraude em concorrência pública.

Dado que os crimes são praticados por atores, estes precisam de informação para a ação, da mesma forma que outros precisam de informação para prevenção e (ou) repressão. Justifica-se, portanto, o emprego de abordagens baseadas em necessidades de informação como estratégia para combate ao crime cibernético.

Necessidades de Informação

Para Silva et al (2002), "a caracterização da necessidade de informação é um campo clássico da Ciência da Informação e da Biblioteconomia". Le Coadic (2004) afirma que "usar informação é trabalhar com a matéria informação para obter um efeito que satisfaça a uma necessidade de informação". De acordo com ele, produtos ou sistemas de informação devem ser orientados para os usuários. Desta forma, conhecer a necessidade de informação permite entender os motivos que levam as pessoas ao processo de busca da informação.

Neste sentido, a compreensão da necessidade de informação está diretamente relacionada à satisfação dos usuários da informação. Contudo, como observa Le Coadic (ibid.), as necessidades têm tipos diferentes. Enquanto umas estão ligadas à obtenção de conhecimento, outras são necessárias para o desenvolvimento de ações. O autor considera duas classes de necessidades de informação, derivadas de necessidades fundamentais:

- A necessidade de informação em função do conhecimento: derivada do desejo de saber.
- A necessidade de informação em função da ação: derivada de necessidades materiais para a realização de necessidades humanas, profissionais e individuais.

Em um mesmo sentido, Rubin (2000) propõe a separação dos tipos de necessidade de informação em desejos de informação e necessidades de informação. O primeiro refere¬se ao desejo de informação para satisfazer uma incerteza e, o segundo, à informação como uma condição em que a informação é necessária para resolver um problema.

Relativamente aos crimes cibernéticos, as necessidades de informação dos agentes nele envolvidos derivam primariamente da função da ação, seja a realização do delito, a prevenção e (ou) repressão. No entanto, sendo a prevenção e a repressão ao crime funções relacionadas à segurança, neste caso manifesta-se o desejo de satisfazer a incertezas, relacionada, portanto, ao desejo de saber e de obter conhecimento.

Estratégia

Existe uma clara diferença entre a informação desejada e a informação necessária para o alcance de um objetivo. Os resultados de estudos da necessidade de informação no combate ao crime cibernético possibilitam não apenas o conhecimento acerca das informações desejadas pelos diversos agentes integrantes do processo criminoso – vítimas, perpetradores e repressores –, mas também o levantamento das informações específicas necessárias à prevenção e à repressão.

> *Temos duas grandes dificuldades. Uma delas ainda é o relativo desconhecimento técnico da Polícia, do Ministério Público, do Judiciário e até mesmo dos advogados de defesa de acusados. A outra dificuldade está na legislação, que impede uma ação rápida da Polícia. No caso dos crimes de informática, a ação rápida é crucial. As evidências digitais são voláteis. O site hoje está no ar, amanhã não está mais (MELO, 2008).*

Além disto, os levantamentos facilitam a conscientização de usuários, a incorporação de práticas à cultura organizacional, bem como o cumprimento de legislações específicas voltada à garantia da segurança no processo interativo de relacionamento via internet, estabelecendo obrigações para os agentes envolvidos.

Santos (2006), em seu artigo "Atual cenário dos crimes cibernéticos no Brasil", cita, como exemplo, a dificuldade de acesso a este tipo de informação em relação às empresas do mercado financeiro.

> *[...] as administradoras de cartão de crédito não divulgam o valor das perdas com fraudes por razões de segurança. Os bancos não têm interesse de comunicar certos roubos para não perder a credibilidade frente aos correntistas e investidores [...] (SANTOS, 2006).*

No momento em que as necessidades de cada ator forem bem conhecidas tornar-se-á mais provável o envio de informações às instituições repressoras relacionadas aos crimes cometidos, independentemente das implicações comerciais ou pessoais que isto possa acarretar.

Agentes Envolvidos

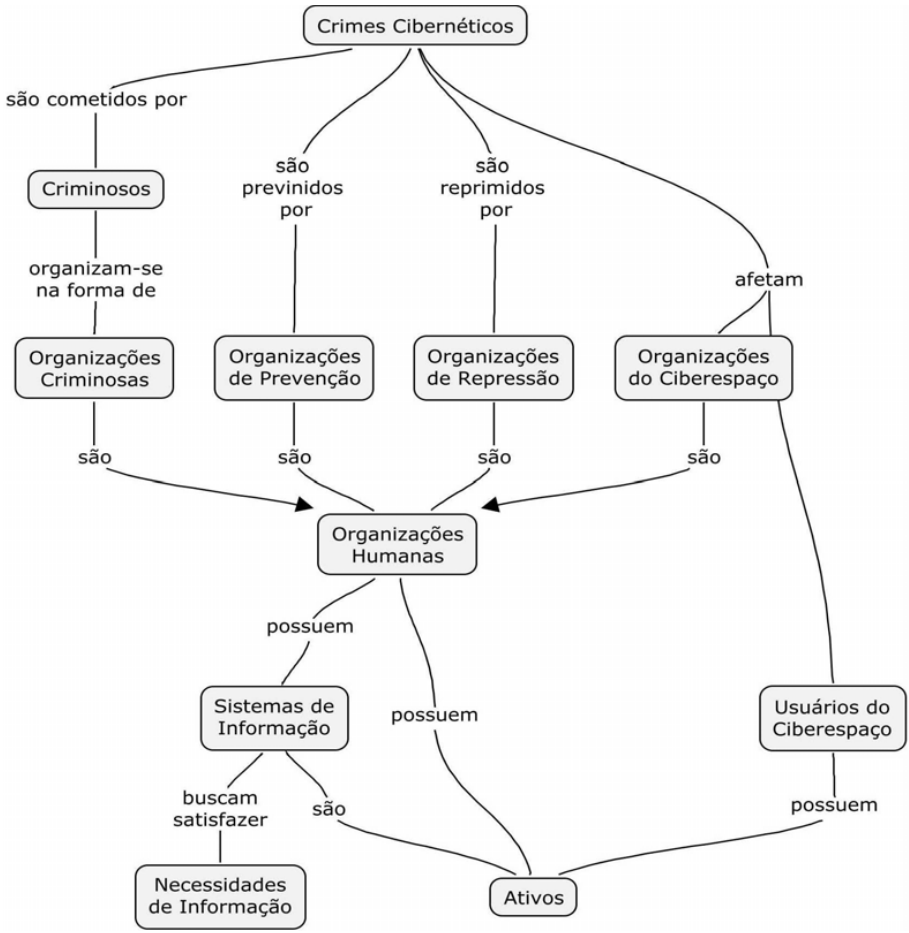

Figura 1 - Atores no domínio do Crime Cibernético.

No processo que envolve a prática de crimes na internet podem-se visualizar diversos elementos. Para a aplicação do estudo da necessidade de informação propõe-se a análise dos cinco principais agentes, que, com objetivos distintos, demandam informações para que suas atividades sejam efetivadas: (i) usuários do ciberespaço; (ii) organizações do ciberespaço; (iii) organizações criminosas; (iv) organizações de prevenção e (v) organizações de repressão.

A Figura 1 apresenta uma relação entre estes agentes por meio da modelagem conceitual através de mapas cognitivos. Das cinco categorias de atores três delas -organizações criminosas, de prevenção e de repressão -adotam postura ativa e duas -usuários e organizações do ciberespaço -são usualmente passivas. Quatro são organizações humanas, e, portanto, possuem capacidade para estruturar sistemas de informação voltados à satisfação das suas necessidades de informação, inclusive às relacionadas ao crime cibernético. No entanto, destas quatro, apenas três possuem funções diretamente relacionadas ao crime cibernético: organizações criminosas, de prevenção e de repressão.

As organizações criminosas atuam visando uma ação lucrativa sobre os usuários e as organizações humanas presentes no ciberespaço e que detém um conjunto significativo de ativos.

Dado o caráter de virtualidade do espaço cibernético, as organizações de prevenção estruturam sua ação principalmente em torno do fornecimento de informações que orientem usuários e organizações do ciberespaço sobre controles que podem ser adotados para evitar sucesso na ação criminosa.

As organizações de repressão combatem o crime cibernético especialmente através do uso da combinação entre inteligência e força, estruturando ações de forma operacional.

Necessidades de Informação dos Agentes no Domínio do Crime Cibernético

Esta seção apresenta uma análise parcial e preliminar de necessidades de informação das cinco categorias de atores no domínio do crime cibernético: (i) usuários do ciberespaço;

(ii) organizações do ciberespaço; (iii) organizações criminosas; (iv) organizações de prevenção e (v) organizações de repressão.

Usuários

Os usuários do ciberespaço empregam a internet como um veículo de convivência com outros 'habitantes', e possuem o conjunto mais difuso de necessidades de informação. Considerando, no entanto, apenas a necessidade referente ao aspecto crime cibernético, esta é derivada do desejo de saber e do conhecimento. Como se trata de uma necessidade básica de segurança, o usuário precisa ser em geral motivado para busca espontânea desta informação ou, de outra forma, já ter sido vítima de crimes cibernéticos. Uma vez motivado, o usuário precisa se proteger por meio do conhecimento: (i) do modus operandi dos criminosos e das organizações criminosas; (ii) do funcionamento, limitações e sobretudo as capacidades de virtualização exibidas pela tecnologia que usa; (iii) sobre o que é lícito e ilícito realizar no ciberespaço, do ponto de vista jurídico e (iv) sobre os mecanismos de segurança dos sistemas tecnológicos que utiliza.

Organizações do Ciberespaço

As organizações que habitam o ciberespaço o fazem porque este apresenta oportunidades para a realização de negócios e prestação de serviços. Para tal, as organizações investem capital em sistemas tecnológicos que são integrados à Internet (sítios web, serviços de informação, comércio eletrônico etc).

Adicionalmente, as pessoas que atuam na organização na condição de usuários de sistemas tecnológicos estabelecem considerável parte da interface da organização com a Internet. Desta forma, todas as necessidades de informação pertinentes aos usuários da internet também se aplicam às organizações.

As organizações apresentam um maior risco de segurança relativamente aos usuários, devido ao fato de que muitos de seus negócios e serviços dependem do contínuo funcionamento de sistemas tecnológicos que expõem considerável superfície de ataque à ação de criminosos na

internet. Esta condição não é em geral tão severa no plano do indivíduo. Por exemplo, os sistemas de comércio eletrônico de empresas possuem em geral um grande número de vulnerabilidades e falhas de programação que precisam ser continuamente monitoradas e controladas. Um grande conjunto de sistemas de TI internos às organizações também influencia diretamente na continuidade da presença das organizações no ciberespaço. Estes sistemas também precisam ser continuamente monitorados no plano interno às organizações, e também estão relacionados a crimes cibernéticos, especialmente a sabotagem. Também é preciso considerar que fraudes, falsificações, pornografia infantil e infração da propriedade intelectual cometidas em organizações, mesmo sem o consentimento de seus dirigentes, também começam a ter responsabilidade subsidiária corporativa. Por fim, é preciso considerar que as interrupções na presença de organizações na internet podem ser decorrência de falhas em sistemas de TI relacionadas ao desenho, implementação, operação e (ou) manutenção de sistemas. Embora não sendo enquadradas como ações criminosas, em alguns domínios de atuação, como sistemas de controle de tráfego, estas interrupções podem provocar ações de responsabilidade civil (indenizatórias).

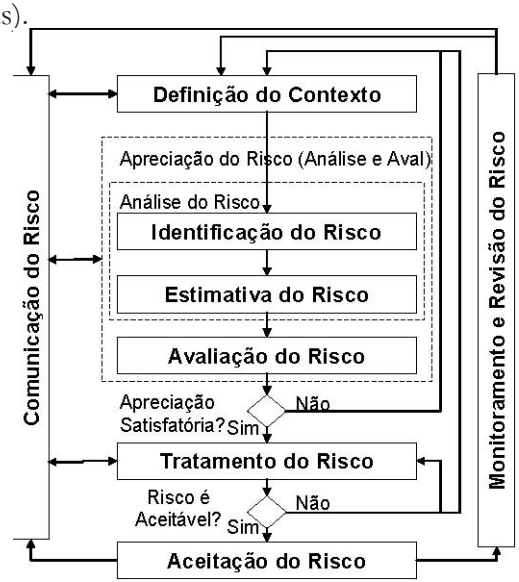

Figura 2. Processo de Gestão de Riscos de Segurança da Informação. Fonte: ABNT ISO/IEC 27005:2008.

Desta forma, a informação fundamental que a organização do ciberespaço deve conhecer é o risco de segurança da informação à qual ela está exposta. Todas as demais informações são articuladas em função do atendimento a esta necessidade. A norma ABNT ISO/IEC 27005:2008 descreve um conjunto de processos que apóiam a gestão de riscos de segurança da informação em organizações. A Figura 2 apresenta uma visão geral destes processos.

Organizações Criminosas do Ciberespaço

As organizações criminosas que habitam o ciberespaço necessitam de informações para lograrem êxito na ação criminosa, isto é, numa ação que lhes seja lucrativa. De forma genérica, o lucro do crime pode ser estabelecido como a diferença entre o investimento para realização da ação e as vantagens auferidas com a mesma. Tais vantagens são relacionadas ao valor dos ativos pertencentes às vítimas potenciais. Desta forma os criminosos as selecionam baseados na relação entre o valor dos ativos e os custos necessários para explorar as vulnerabilidades que permitem o acesso a tais ativos. Quanto maior for o volume de informação acerca dos ativos e das vulnerabilidades das vítimas potenciais -sejam elas usuários ou organizações -mais eficaz e rentável poderá ser a ação criminosa. São exemplos de ativos os dados pessoais de usuários, que permitem o roubo de identidade, e os dados confidenciais das organizações, que permitem práticas de concorrência desleal. São exemplos de vulnerabilidades as falhas nos sistemas de segurança e aplicativos de software empregados pelas organizações, e detalhes pessoais sobre o perfil e comportamento dos usuários do ciberespaço.

Organizações de Prevenção ao Crime Cibernético

Como já mencionado anteriormente as organizações de prevenção ao crime cibernético necessitam de aprofundamento da compreensão das necessidades de informação gerais dos atores analisados nas subseções 6.1, 6.2 e 6.3, e, de posse destas informações, prover orientações

gerais aos usuários e organizações do ciberespaço, de modo que estas se defendam das ações criminosas.

A necessidade de informação dessas organizações está relacionada, portanto, à compreensão da dinâmica geral do crime cibernético, consideravelmente influenciada pelo fluxo de informações que satisfazem às necessidades aqui analisadas.

Organizações de Repressão ao Crime Cibernético

As organizações de repressão ao crime cibernético necessitam de informações similares às demandadas pelas de prevenção, só que com um maior nível de especificidade. De posse destas informações, será possível o planejamento e realização de operações.

A necessidade de informação dessas organizações está relacionada, portanto, à compreensão da dinâmica atual e real do crime cibernético.

Conclusões e Trabalhos Futuros

Conclusões

O estudo da necessidade de informação dos agentes envolvidos no crime cibernético viabiliza o conhecimento acerca do contexto no qual é realizada esta prática. Com isto, é possível a determinação de medidas de antecipação e repressão ao crime, com a integração e a criação de canais de comunicação voltados ao compartilhamento de informações necessárias às entidades envolvidas no processo interativo via internet.

Este conhecimento facilitará a criação de medidas preventivas que dificultem a atuação dos criminosos contribuindo para a determinação de ações padronizadas nos âmbitos jurídico, com a concepção de legislação específica, e operacional.

Trabalhos Futuros

Visando aprofundar a análise de necessidades dos atores no domínio do crime cibernético, uma atividade futura será utilizar o modelo do ciclo de vida da informação descrito na Figura 3 composto por sete fases: (i) a criação da informação ocorre quando algum agente produz uma interpretação de algum fenômeno e registra esta interpretação em algum meio permanente; (ii) o registro é coletado por algum agente interessado no uso futuro da informação; (iii) as informações são organizadas conforme algum esquema de classificação, como uma taxonomia, tesauro ou ontologia, explicita ou implicitamente definida; (iv) o registro é armazenado em meio permanente, usualmente empregando computadores digitais; (v) a informação é distribuída dentro de uma rede integrada ao sistema de informação; (vi) a informação é buscada por algum usuário que dela necessita; (vii) o usuário tem acesso ao registro e assim recupera a informação para alguma finalidade. A contínua necessidade da informação dentro de organizações é responsável por fomentar a criação e manutenção de sistemas que apóiam o funcionamento de ciclos desta natureza dentro das organizações.

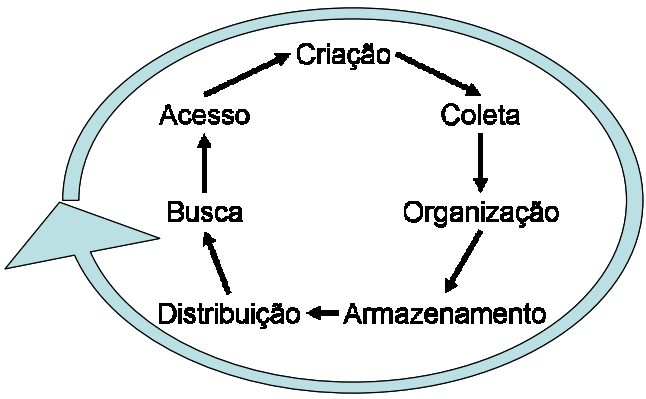

Figura 3 – Um Ciclo de Vida da Informação em Sistemas de Informação.

Por meio da aplicação deste modelo estimamos ser possível identificar novas necessidades de informação, bem como aprofundar a com-

preensão das já indicadas. O ciclo torna possível a concepção de uma perspectiva sistêmica, levando ao aprofundamento dos processos e sistemas empregados pelas organizações de prevenção e repressão aos crimes cibernéticos.✍

FELIPE LOPES DA CRUZ

Departamento de Ciência da Informação – Universidade de Brasília (UnB). Campus Universitário Darcy Ribeiro – 70.919-970 – Brasília – DF – Brazil

E-mail: felipelopes@unb.br

JORGE HENRIQUE C FERNANDES

2Departamento de Ciência da Computação – Universidade de Brasília (UnB). Campus Universitário Darcy Ribeiro – 70.919-970 – Brasília – DF – Brazil.

E-mail: jhcf@cic.unb.br

ABSTRACT

Measures deemed to intimidate cybercriminals are justified due to the growth and negative impact of such activities to the information society. The rise of cybercrime, among other factors, is due to the lack of specific legislation that characterize this kind of crime and also due to some vulnerabilities existent in IT security systems. This paper presents preliminary results from the application of a study about information needs of the actors involved in cyberspace. More specifically the information needs of users, organizations, cybercriminals and organizations that prevent and combat the cybercrime were analyzed. The paper argues this is a strategy to anticipate, prevent and combat the rising crime rates in the cyberspace.

Keywords: Information. Strategy. Cybercrime.

Referências

COE - Council of Europe. *Convention on Cybercrime*. Budapest. 23.XI.2001. Available

URL: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm. Last accessed in

Dec 2008.

LE COADIC, Yves-François. *A ciência da informação*. 2. ed. Brasília: Briquet de Lemos, 2004.

MELO, Leonardo Bueno. *Batalha digital:* Falta de lei e de informação beneficiam o cibercrime. Disponível em: http://www.conjur.com.br/static/ text/68250,1#null. Acesso em: 05/12/2008.

PERRIN, Stephanie. *O cibercrime.* Disponível em: http://vecam.org/article660.html. Acesso em: 07/12/2008.

RUBIN, Richard E. *Foundations of library and information science*. United States: Neal-Schuman Publishers, Inc. 2000.

PINHEIRO, Emeline Piva. *Crimes Virtuais:* Uma análise da criminalidade informática e da resposta estatal. Disponível em: http://www.pucrs.br/uni/poa/direito/graduacao/tc/tccII/trabalhos2006_1/emeline.pdf. Acesso em: 05/12/2008.

SENADO FEDERAL. *SF PLS 00076/2000 de 27/03/2000*. Define e tipifica os delitos informáticos, e dá outras providências. http://www.senado.gov.br/sf/ATIVIDADE/materia/Detalhes.asp?p_cod_mate=43555 Último acesso em dez 2008.

SANTOS, Coriolano Aurélio Almeida Camargo. *Atual cenário dos crimes cibernéticos no Brasil.* Disponível em: http://www2.oabsp.org.br/asp/comissoes/sociedade_informacao/artigos/crimes_ciber neticos.pdf. Acesso em: 06/12/2008.

SILVA, Janete F.; FERREIRA, Marta A. T.; SOUZA, Mônica E. N. *Análise metodológica dos estudos de necessidades de informação sobre setores industriais brasileiros:* proposições. Ciência da Informação, Brasília, v. 31, n. 2, p. 129-141, maio/ago. 2002. Disponível em: http://www.scielo.br/pdf/ci/v31n2/12916.pdf. Acesso em: 09/02/2008