TERRORISMO CIBERNÉTICO E CENÁRIOS ESPECULATIVOS

Tecnologista Sênior Eduardo Müssnich Barreto
Abin

A expressão **Terrorismo Cibernético** diz respeito ao emprego, por terroristas, de técnicas de destruição ou incapacitação de redes computacionais de informação. Entre essas redes, destaca-se a internet, em razão do seu crescente fluxo de informações, importância, abrangência e extensão geográfica.

O mundo não conhece, até o presente, exemplos de atentados terroristas cibernéticos, apesar de já colecionar uma infinidade de eventos ilícitos cometidos por intermédio das redes de computadores, na forma de **ataques cibernéticos** contra bancos, empresas, órgãos governamentais e indivíduos em todo o mundo. Por isso, especialistas em Terrorismo Cibernético costumam apoiar-se na concepção de cenários possíveis, mediante avaliações feitas a partir da quantificação das (1) **vulnerabilidades** conhecidas e existentes nos sistemas informatizados, das (2) **ameaças** hipotéticas e reais que sobre eles incidem, e, finalmente, do (3) **valor** estratégico, político ou econômico das informações operadas nesses sistemas.

Em sua concepção popular mais comum, o atacante de sistemas informatizados é um jovem adolescente que pratica um ataque individual. Para o estudo do Terrorismo Cibernético, entretanto, tal conceito vem sendo ampliado, uma vez que os efeitos pretendidos buscariam impactos de longo prazo nos planos psicológico, econômico ou da segurança da população. As ações de resposta, por sua vez, deverão ser coordenadas no âmbito governamental, sob complexo gerenciamento e legislação específica. Dessa forma, o terrorista cibernético deve ser entendido não como um indivíduo, mas um **grupo,** suficientemente coordenado, especializa-

do, inteligente e disciplinado, com expressivos recursos financeiros, materiais, e disponibilidade de conhecimento e tempo. Naturalmente, a proteção contra *hackers* individuais deve ser sempre considerada, mas mantém-se importante analisar e prevenir a ameaça maior representada por adversários detentores de significativo e organizado potencial destrutivo.

Ainda para os propósitos de estudo, é relevante considerar que o Terrorismo Cibernético deverá empregar técnicas similares às utilizadas na **Guerra Cibernética**, na qual o conflito ocorre entre Estados no plano militar.

A dependência da Tecnologia da Informação e das Comunicações

A **Tecnologia da Informação e das Comunicações (TIC)** desempenha papel crítico na gestão e operação de sistemas, como os de telecomunicações, geração e distribuição de energia, controle aéreo, instituições financeiras, defesa, logística e abastecimento de bens, água e alimentos. Sistemas dessa natureza compõem as denominadas **infra-estruturas críticas**, dotadas de diferentes graus de vulnerabilidade frente a ataques de terceiros.

A crescente dependência dos setores estatal e privado mundiais a esses sistemas, assim como sua criticidade é conseqüência natural dos avanços tecnológicos e de confiabilidade das aplicações de TIC.

Tipos de ataque a infra-estruturas TIC

Qualquer infra-estrutura TIC poderia ser **alvo** de uma ação terrorista. Um exemplo seria a paralisação do sistema de controle de tráfego aéreo de um aeroporto importante. Por outro lado, a infra-estrutura TIC poderia ser, não mais o alvo, mas a **ferramenta** utilizada em um ataque, como uma intencional alteração de dados de vôo que objetivasse produzir um acidente aéreo.

De forma genérica, um ataque a uma infra-estrutura TIC poderia receber a seguinte classificação:

a) ataque técnico;
b) destruição física; e
c) pessoa infiltrada *(insider)*.

Um **ataque técnico** poderia ocorrer na forma de um programa *(software)* ilícito, a exemplo dos vírus, cavalos-de-tróia, Distributed Denial-of-Service (DDoS) e até mesmo sistemas operacionais. Os **vírus** de computador já causam prejuízos mundiais crescentes em termos de tempo e custos de reparação. Como exemplo, o notório vírus ***I Love You***, de acordo com o Federal Bureau of Investigations (FBI), teria provocado dano estimado em U$ 10 bilhões à economia estadunidense. Os **cavalos-de-tróia**, por sua vez e de forma sucinta, são programas que permitem a terceiros de má-fé o acesso a informações armazenadas em sistemas remotos. Sua modalidade mais popular e agressiva são os *spybots*, uma instalação clandestina que costuma ser realizada pela própria vítima, desinformada sobre riscos, ao clicar determinadas figuras ou *links* em e-mails recebidos. Já os **DDoS**[1] são ataques coordenados que sufocam o site-alvo com uma infinidade de pedidos de acesso simultâneos, deixando o usuário legítimo sem atendimento no momento de sua necessidade. Todas essas ameaças exploram sérias vulnerabilidades inerentes à internet, cujos protocolos de comunicação foram criados ainda na década de 1960, quando a atual internet sequer era imaginada, menos ainda seu uso para fins ilícitos.

Um outro tipo de ataque técnico envolve os **sistemas operacionais** (a exemplo do Linux, Windows e Unix). Tais *softwares* controlam integralmente a operação de computadores. Uma das modalidades de ataque consiste em uma modificação provocada

1 Em fevereiro de 2000, repetidos ataques do tipo DDoS (Distributed Denial-of-Service) perpretados durante quatro dias desabilitaram os sites Yahoo, Amazon, E*Trade, eBay, CNN.com e outros. Apesar de as empresas alegarem baixos prejuízos financeiros, o governo federal estadunidense reuniu especialistas para discutir as vulnerabilidades presentes na internet. As investigações custaram milhões de dólares, despertando grande interesse da opinião pública.

no sistema operacional, de forma que este passe a reconhecer o acesso do atacante e privilegie-o com permissões especiais, garantindo que seu trânsito no sistema seja absolutamente livre, inclusive não-rastreável pelas rotinas de auditoria. Essa modalidade não é hipotética, sendo há muito utilizada por *hackers* e popularmente conhecida como ***rootkit.***

Eventualmente, uma das quatro novas falhas descobertas a cada dia, em média, nos sistemas operacionais existentes no planeta representa uma séria **vulnerabilidade** passível de exploração por atacantes. Essas vulnerabilidades são a matéria-prima utilizada pelos *hackers*. Daí decorre uma outra modalidade de ataque, ainda mais grave e oculta, que poderia ocorrer ainda durante a fase de desenvolvimento do sistema operacional, em que rotinas clandestinas especiais conteriam mecanismos para se realizar transferência de informações para terceiros, ou mesmo desabilitar completamente, caso oportuno, os sistemas críticos em operação. Muitos sistemas operacionais comerciais são inauditáveis até o presente, uma vez que seus códigos-fonte não são disponibilizados pelos fabricantes. Sob tal análise, poder-se-ia inferir serem tais sistemas operacionais (ditos "fechados") ferramentas dotadas de eficácia potencial para emprego por forças armadas ou serviços de Inteligência adversos. Por exemplo, uma determinada chave criptográfica embutida secretamente em um sistema operacional poderia viabilizar o rompimento remoto de seus mecanismos naturais de segurança, como senhas e controle de portas lógicas.

A segunda classe de ataques, a **destruição física,** seria executada contra componentes da infra-estrutura, como centrais, equipamentos e conexões. A expectativa do terrorista seria infligir a indisponibilidade dos sistemas críticos, que poderia durar horas ou dias, além de criar o receio na população de que novos incidentes poderiam ocorrer a qualquer momento. No caso brasileiro, alguns desses componentes encontram-se fora do território nacional e do controle estatal, a exemplo do sistema Domain Name System

(DNS)[2], essencial à operação da internet e localizado no território estadunidense.

A terceira classe, **infiltração de pessoas** (*insiders*), objetiva, entre outros:

1 - disponibilização de **senhas** (obtidas inclusive com o emprego de cavalos-de-tróia) que permitirão o acesso externo de terceiros não-autorizados;

2 - instalação prévia de **programas hostis** que produzam ou facilitem o ataque; e

3 - **modificações de hardware**.

A exemplo disso, no início da década, descobriu-se que um programador de sistemas navais do Japão repassara senhas de acesso às redes de computadores a integrantes da seita extremista Aum Shinrikyo, a mesma responsável pelos ataques com gás sarin no metrô de Tóquio, em 1994.

Naturalmente, ataques que contam com o acesso de *insiders* são mais difíceis de executar, por não serem pessoas de confiança para nenhum dos lados, e, logo isso, por serem menos prováveis de ocorrer. Mas é relevante mencionar que os casos de espionagem mais relevantes da história recente envolveram *insiders*, como Aldrich Ames e Robert Hanssen.

Danos possíveis às infra-estruturas de TIC

Os especialistas concordam que a obtenção da **segurança total** dos sistemas críticos de TIC, ligados ou não à internet, é consi-

[2] O sistema denominado Domain Name System (DNS) realiza a tradução de cada nome de domínio (por exemplo, www.dominio.com.br) para os endereços de IP (Internet Protocol) (por exemplo: 200.27.81.127) que identificam cada "nó de rede" específico na internet. Embora o DNS tenha sido projetado com redundâncias, é considerado vulnerável frente a um ataque simultâneo a seus servidores, e sua indisponibilidade pode ocorrer por vários dias.

derada **impossível**. As ações de segurança buscam tão somente identificar, controlar e reduzir as vulnerabilidades existentes, além de minimizar os possíveis efeitos de um eventual ataque.

Os danos causados às infra-estruturas recaem sobre três categorias elementares, podendo ocorrer em simultaneidade:

1 – **indisponibilidade** - nesse caso, os sistemas deixam de responder dentro de prazos oportunos;

2 – **adulteração de informações** - as respostas deixam de ser confiáveis, por terem sido alteradas; e

3 – **acesso não-autorizado** - os sistemas permitem que terceiros (pessoas ou computadores) não-autorizados acessem informações privilegiadas, ou obtenham o próprio controle operacional do sistema.

Componentes da infra-estrutura de TIC

A infra-estrutura de TIC, por sua vez, poderia ser contextualizada como possuidora de cinco componentes básicos, cada um com vulnerabilidades próprias frente a ataques cibernéticos, como será visto mais adiante:

1 – a internet;

2 – as redes de telecomunicações;

3 – os sistemas de controle em tempo real, como os empregados em controle de tráfego aéreo e distribuição de energia, bem como o sistema financeiro;

4 – os sistemas de produção, de comercialização e de prestação de serviços; e

5 – os sistemas especiais, de essência estratégica.

• Componente 1 – a internet

A internet interconecta diversas redes mediante um protocolo comum de comunicação. O roteamento (encaminhamento) dos pacotes de comunicação na rede é realizado de forma eficiente e automática, cabendo ao protocolo escolher, para a transmissão dos dados, as vias e áreas menos congestionadas e mais

confiáveis. Dessa forma, um grande número de “nós de rede” precisaria ser simultaneamente destruído para que a internet ficasse indisponível por um longo período.

Apesar das facilidades disponibilizadas pela internet, muitas organizações não lhe confiam suas operações de negócios, mantendo processos alternativos de comunicação. Por exemplo, há notícias de que, desde 5 de dezembro de 2001 (três meses após o atentado ao World Trade Center), o próprio Departamento do Interior dos Estados Unidos tem operado, em grande parte, fora da internet, por razões de segurança e independência operacional, usando *modems* e fax, alegadamente sem grande prejuízo de sua eficiência.

Meses antes, em 19 de julho de 2001, o *worm* denominado ***Code Red*** infectara perto de 360.000 computadores em menos de 14 horas. Em 18 de setembro do mesmo ano, o vírus ***Nimda*** atingia 150.000 servidores *web* e computadores nos EUA, causando expressiva lentidão nas redes corporativas. Estima-se que ambos tenham causado prejuízos mundiais da ordem de 3 bilhões de dólares em perda de produtividade, reinstalações, limpeza e testes de sistemas.

• Componente 2 – as redes de telecomunicações

A redundância presente nas redes de telecomunicações é significativamente menor que a existente na internet. Um ataque ou falha em um grande centro de comutação telefônica ou de dados poderia romper as comunicações entre regiões geográficas por tempo considerável.

Uma cidade possui diversos centros de comutação distribuídos, o que acrescenta complexidade a um ataque. Entretanto, a destruição cirúrgica de centros associados a agências governamentais, centros financeiros, e instalações críticas ou de emergência (polícia, bombeiros, hospitais) potencializaria os efeitos de uma ação terrorista maior e coordenada.

• Componente 3 – os sistemas em tempo real

Muitos sistemas computacionais, mesmo aqueles pré-implantados e que não permitam a atualização de seu *software*, podem ser corrompidos com o passar do tempo. Classificam-se aqui, por exemplo, os equipamentos de controle empregados em aeronaves (denominados aviônicos), que são passíveis de ataques precedidos da infiltração por um programador especializado (*insider*), ainda na fase de desenvolvimento dos sistemas.

Os riscos maiores, entretanto, estão nos sistemas TIC que controlam **infra-estruturas críticas** de importância local, regional ou nacional, a exemplo de:

1 - malha elétrica;
2 - sistema de controle de tráfego aéreo;
3 - rede financeira;
4 - purificação e distribuição de água;
5 - infra-estrutura de transportes;
6 - sistemas governamentais; e
7 - redes de notícias.

A **malha elétrica** tem uma característica de vulnerabilidade que a diferencia dos demais itens citados: é possível que uma falha em uma região geográfica se propague para outras, por efeito cascata, produzindo dimensões e danos consideráveis antes que possa ser corrigida.

Um ataque técnico contra um segmento da malha elétrica poderia resultar em dano comparável ao de um “apagão”. Ao utilizar a falta de energia em seu proveito, entretanto, terroristas poderiam infligir outros ataques físicos com maior impacto do que seria possível sem o caos implantado pelo ataque inicial. Esse mesmo ataque, por sua vez, poderia provocar um efeito cascata de desligamentos e impedir o fornecimento de energia a grandes extensões geográficas por longo tempo. Os efeitos dessas interrupções são de difícil previsão, tanto por parte dos operadores quanto dos atacantes.

Apesar da natural vulnerabilidade do sistema elétrico representada pela possibilidade de destruição física das torres de transmissão, o risco real de um ataque cibernético é maior nos países mais desenvolvidos, onde o controle do sistema é feito por redes computacionais de supervisão.

A consciência de segurança nas redes cibernéticas que apóiam **sistemas financeiros nacionais** é muito grande, o que as torna menos vulneráveis. Em razão de sua sensibilidade, os sistemas centrais (a exemplo do Banco Central) e de transações de alto volume normalmente empregam redes distintas dos sistemas públicos, de forma que o êxito em ataques a tais sistemas necessitaria, assim se prevê, de significativo acesso infiltrado (*insider*). A exemplo disso, o sistema financeiro central brasileiro, objetivando redundância, emprega atualmente dois sistemas em paralelo, simultaneamente disponíveis a seus usuários.

Por outro lado, os sistemas financeiros periféricos costumam ter menor redundância; além disso, uma parte de suas redes de telecomunicações, por razões de economia, é compartilhada com as redes públicas contratadas em concessionários de comunicações. Dessa forma, tornam-se vulneráveis a interrupções de serviços em grande escala e até mesmo a eventuais ataques à infra-estrutura de telecomunicações.

Os **sistemas governamentais** permitem transações de governo, como as de planejamento, orçamento, arrecadação, despesa, controle interno e externo, defesa civil e militar, saúde, previdência e assistência social, entre outros.

Uma parte das estruturas de governo em todo o mundo vem contratando serviços terceirizados de suporte técnico, e, em alguns casos, a terceirização é absoluta, envolvendo desde o projeto dos sistemas, sua instalação, operação, manutenção e armazenamento de dados, até as decisões estratégicas periodicamente demandadas no setor de TIC. Do ponto de vista de segurança, tais empresas podem servir de canal de entrada para *insiders* ligados ao terrorismo.

A **infra-estrutura de transportes** abrange portos, aeroportos, trens, metrôs e é responsável pelo deslocamento seguro e eficiente de pessoas e cargas, incluindo alimentos e combustíveis. Nos países desenvolvidos, o controle dessas infra-estruturas é crescentemente apoiado em sistemas TIC.

Quanto às **redes de notícias,** o terror poderia ser difundido na população mediante desinformação, a exemplo da divulgação de uma falsa informação sobre uma determinada ameaça.

- **Componente 4 – os sistemas de produção, comercialização e de prestação de serviços**

Os sistemas produtivos contam pesadamente com a disponibilidade e confiabilidade das TIC. As conexões existentes entre computadores e a internet permitem meios possíveis para ataques a setores funcionalmente relevantes para diversos setores da economia. Entre os meios amplamente utilizados, poderiam ser citados: a atualização de sistemas operacionais; e a disponibilização de programas *shareware*, a exemplo do compartilhamento de arquivos de música.

É relevante notar que os sistemas dotados de *firewalls* e dispositivos similares possuem melhor grau de proteção que os demais; entretanto, de acordo com registros recentes, tais medidas não garantem que terceiros não-autorizados não possam penetrá-los.

A par do ataque técnico já citado, que envolveria ferramentas do tipo cavalos-de-tróia e vírus, os grupos de estudo sobre o assunto também desenvolvem uma preocupação crescente acerca do *insider*. Isso porque organizações terroristas poderiam usá-los nas empresas de desenvolvimento de *software* e *hardware*, e introduzir **funcionalidades não-autorizadas** nos sistemas de amplo emprego, como microcomputadores e servidores padronizados de uso genérico. No caso, os alvos de ataque mais prováveis seriam aqueles computadores de instituições usuárias (empresas e até mesmo órgãos de governo) de alta sensibilidade, a exemplo de empresas de tecnologia de ponta ou ainda organismos de segurança e/ou Inteligência.

• **Componente 5 – sistemas especiais**

Uma categoria de sistemas bastante sensível a ser também considerada é aquela formada por sistemas estratégicos, incluindo os de defesa. São sistemas de comercialização bastante restrita e com fortes controles internacionais, como os de armas, navegação aeroespacial e marítima, vigilância aérea e meteorologia.

Tais sistemas são freqüentemente adquiridos de um pequeno grupo de países que detêm a tecnologia mais competitiva e eficaz. Eles incorporam sistemas operacionais, de comunicações e de segurança criptográfica, todos quase completamente baseados em *software*. Pode-se constatar, aqui, a vulnerabilidade já citada e bastante conhecida dos programadores de *software*: a facilidade de esconder comandos clandestinos em programas de computador. Considerando-se que tais equipamentos e sistemas dedicados são governados exclusivamente por comandos de *software*, seria possível a inserção de comandos não-documentados (ainda que ausentes dos manuais técnicos e das especificações) que tornariam possível a terceiros (mais exatamente, a seus próprios programadores ou aliados) **desabilitar ou alterar a operacionalidade** daqueles sistemas em um momento específico.

Se uma organização terrorista, por exemplo, fosse capaz de provar haver corrompido o *software* de controle de uma aeronave civil de grande porte e que poderia derrubá-la sob demanda, a confiança pública na indústria da aviação seria abalada, e o sistema de aviação poderia ser paralisado até que uma completa auditoria fosse realizada e o *software* de controle validado.

Seguindo essa lógica, haveria ainda a possibilidade de **desligamento** ou indução de erros em sistemas de localização, como o Global Positioning System (GPS). Apesar de o GPS ser disponibilizado em regime precaríssimo (uma vez que não confere qualquer direito ou garantia a seus usuários), muitos sistemas especiais, e até mesmo alguns que integram infra-estruturas críticas, dependem das informações fornecidas pelo GPS público. Uma vez desabilitado ou modificado, os diversos sistemas que

nele se apóiam ficariam instantaneamente indisponíveis ou em erro, respectivamente.

Um outro exemplo seria o de um míssil que, em curso contra seu alvo, verificaria repetidamente (mediante instrução interna não constante dos manuais) a existência de determinado código sendo transmitido a uma específica freqüência eletromagnética: se o código fosse identificado, o míssil entenderia que seu curso deveria ser alterado. O que poderia parecer uma falha fortuita do equipamento, tratar-se-ia na verdade de uma **avaria planejada,** concebida na fase de projeto do equipamento. O mesmo poderia ocorrer com aviões-caça, radares, sistemas de comunicações e de telemetria, equipamentos para veículos lançadores de satélites, assim como os próprios satélites, todos demandando, da parte dos países adquirentes, a realização de processos de **auditoria** prévia de sistemas para verificação da legitimidade dos *softwares* neles embutido.

Quanto a tais sistemas estratégicos, a pergunta poderia ser: "como garantir que este sistema estará operacional no momento em que se tornar indispensável?".

Conclusão

Em regra, as ameaças mais prováveis serão aquelas que envolverem ataques simples contra alvos complexos. Um pequeno mas experimentado grupo de *hackers* teria condições de infligir danos à infra-estrutura crítica e à credibilidade pública. O ataque cibernético, por sua vez, em razão de reduzida repercussão visual na mídia, não produziria o pânico imediato e não geraria imagens de fogo e destruição. Mesmo assim, poderia ser empregado como **multiplicador de efeitos**, ao potencializar os danos causados por um ataque físico, mediante obstaculização ou desinformação.

Caso haja apoio de retaguarda de um Estado adversário, com recursos financeiros e técnicos suficientes, um ataque poderia ser ainda maior, mais coordenado e prolongado. E poderia também,

se executado de forma sistemática, corromper uma produção de *hardware* ou *software*, como visto acima. Considera-se ainda que repetidos ataques contra a internet poderiam causar efeitos que prejudicariam as tentativas de reparo do primeiro ataque.

Se forem usados vírus de computador muito provavelmente serão novos vírus, imunes aos programas antivírus existentes. Por isso, é provável que um eventual ataque seja rápido. A existência de redes internacionais de **equipes de resposta a incidentes** tem aqui sua maior importância: ao passo que reforçam a infra-estrutura de prevenção, detecção e resposta, esses núcleos especializados terão os meios de produzir, de forma oportuna, as iniciativas de recuperação dos sistemas atingidos.

A grande dificuldade em prever-se, com precisão, o momento e a forma como se dará um ataque terrorista induz à noção da necessidade de **planos de contingência**, nos quais constem, entre outros, as responsabilidades, as medidas básicas assecuratórias do rápido restabelecimento dos serviços prejudicados, a gestão dos riscos operacionais e, importante, o plano de comunicação a ser adotado. Além do regular armazenamento de cópias de segurança dos dados (*backups*) em locais distribuídos, as entidades que dependem, de forma crítica, de sistemas computacionais já vêm optando por instalações computacionais e de comunicações em duplicidade.

Assim, as ações de segurança buscam tão-somente identificar, controlar e reduzir as vulnerabilidades existentes, além de minimizar os possíveis efeitos de um ataque. As partes sensíveis dos planos de contingência, que identificarem vulnerabilidades organizacionais, deverão ser protegidas contra o acesso dos atacantes e receber **tratamento sigiloso**.

Apesar das consideráveis dificuldades administrativas, financeiras, culturais e até mesmo legais envolvidas, os países centrais atualmente buscam a implementação da **Gestão da Segurança da Informação** em seus órgãos e empresas. Tal solução já conta com um padrão internacional, da série ISO, convertido em uma

norma brasileira em 2001, a NBR ISO/IEC 17799, e envolve a nada simples tarefa de conscientizar usuários e tomadores de decisão, em todos os níveis, das necessidades de práticas eficazes, de contramedidas, auditorias de gestão de pessoal, *hardware* e *software*, critérios de contratação de empresas e de seleção de pessoal terceirizado, enfim, alcançar as necessárias e suficientes **percepções** que permitam solver os inéditos desafios de segurança formulados, a cada novo dia, pela Tecnologia da Informação e das Comunicações.

Cabe, ainda, registrar a opinião de um segundo grupo de especialistas em segurança, que entende serem exageradas as possibilidades de uso das TIC por grupos terroristas acima mencionadas. Em sua visão, a complexidade das tarefas e o resultado pouco aparente dos efeitos do Terrorismo Cibernético seriam de reduzido interesse àqueles grupos, que teriam, à sua disposição, diversas outras mais simples e efetivas fórmulas de produção de danos, vítimas e medo.

Referências

COMMITTEE ON THE ROLE OF INFORMATION TECHNOLOGY IN RESPONDING TO TERRORISM. **Information technology for counterterrorism:** immediate actions and future possibilities. Washington, D.C.: National Academy Press, 2003. 128 p.

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD. **Cybersecurity today and tomorrow:** pay now or pay later. Washington, D.C.: National Academy Press, 2002. 40 p. Disponível em: <http://www7.nationalacademies.org/CSTB/prepub_cybersecurity.pdf>

CONFERENCE ON INTERNATIONAL COOPERATION TO COMBAT CYBER CRIME AND TERRORISM, 1999, Stanford, California. Stanford: Stanford University,1999.

SOAFER, Abraham D.; GOODMAN, Seymour E. **The transnational dimensions of cyber crime and terrorism.** Stanford, CA.: Hoover Institution Press, 2001. 292 p.

WORKSHOP ON TERRORISM IN A HIGH-TECH SOCIETY AND MODERN METHODS FOR PREVENTION AND RESPONSE, 2001, Moscow, Russia**. High-impact terrorism: proceedings of a Russian-American workshop.** Washington, D.C.: National Academy Press, 2002. 279 p.

* * *

EM DEFESA DO BRASIL