O PAPEL DO SERVIÇO DE INTELIGÊNCIA NA SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS

Fábio Nogueira*

Resumo

Danos a infraestruturas críticas geralmente têm impactos negativos de grande monta na vida das pessoas. Ao Estado cabe liderar o processo de proteção desses ativos e ao Serviço de Inteligência compete cooperar com os órgãos responsáveis. O artigo decompõe em quatro fases o processo de proteção das infraestruturas críticas e indica em que pontos a Inteligência pode contribuir para esta segurança.

1 Introdução

Um incêndio nas instalações de uma operadora de telecomunicações em dezembro de 2010 provocou a interrupção, por pelo menos uma semana, de serviços de telefonia fixa, móvel e acesso a internet, afetando a vida de muitos consumidores baianos. Milhares de chineses já morreram em acidentes na exploração de minérios, como na província de Xinfen na Mina de Tashan, em setembro de 2008, em que 254 trabalhadores vieram a óbito após o desabamento de resíduos e pedras por causa da chuva. No Maranhão, a explosão do Veículo Lançador de Satélites (VLS-1) em agosto de 2003 gerou atraso no cronograma de desenvolvimento do programa espacial brasileiro, causando a morte de 21 técnicos altamente qualificados. Um dos maiores desastres ambientais aconteceu em março de 1989 no Alasca, onde um acidente com o petroleiro Exxon Valdez provocou o derramamento de aproximadamente 42 milhões de litros de óleo cru.

Seja em pequena ou grande escala, recentemente ou há décadas, implicando em mortes ou não, em países desenvolvidos ou em desenvolvimento, os sinistros abrangendo uma infraestrutura indispensável à nação acarretam inúmeros prejuízos, de vidas ou patrimonial. A população que experimenta os danos e transtornos almeja tão somente que o problema não se repita, além do desejo de ter o pronto restabelecimento do serviço. Portanto, é necessário que se resguarde a integridade dos ativos es-

* Bacharel em Ciência da Computação (UFV, MG). Especialização em Gestão Estratégica com Ênfase em Qualidade e Competividade (UFMG). Mestrado Profissional em Administração (PUC/MG).

senciais, ditos críticos, para a população usuária desses bens e serviços, e que se tenham planos para retomar a operação imediatamente. Cabe ao Estado, por meio de sua estrutura técnica e de segurança, incluindo a Inteligência, liderar um programa de proteção.

Mas afinal, o que é Infraestrutura Crítica (IC)? A Portaria nº 02, de 08 de fevereiro de 2008, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) (BRASIL, 2008), definiu o termo como "as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional". Além disso, agrupou as ICs em cinco áreas prioritárias: energia, transporte, água, telecomunicações e finanças.

Em outros países verifica-se a mesma linha de pensamento. Na França (2006), IC foi definida, por meio do decreto nº 2006-212 de 23 de fevereiro de 2006, como "todas as infraestruturas que são vitais para a manutenção dos principais processos sociais e econômicos". Os setores críticos são: finanças, indústria, energia, o trabalho do Judiciário, da Saúde Pública, das autoridades nacionais civis, comunicação eletrônica, mídia audiovisual e tecnologia da informação, sistemas de transportes, abastecimento de água, alimentação, espaço e pesquisa, e Forças Armadas. Na Austrália, para o *Attorney-General´s Department*[1], autoridade responsável pela elaboração da Estratégia de Resiliência das Infraestruturas Críticas, a definição de IC são "as instalações físicas, cadeias de suprimento, tecnologias de informação e redes de comunicação que, se destruídos, degradados ou tornados indisponíveis por um período prolongado, teria um impacto significativo sobre o bem-estar social e econômico da nação, ou afetar a capacidade de defesa nacional da Austrália e garantir a segurança de seus habitantes". Os setores de IC são: finanças, comunicações, energia, alimentos, saúde, transporte e serviços de abastecimento de água (AUSTRÁLIA, 2010).

Os Estados Unidos (EUA), um dos pioneiros na tarefa de proteger ICs, primeiramente definiu o termo, a partir da Comissão Presidencial de Proteção de Infraestrutura Crítica (PCCIP) em 1996, como infraestruturas tão vitais que sua incapacitação ou destruição teria um impacto debilitador na segurança econômica ou de defesa da nação. Mais tarde em 2001, sob efeito dos eventos de 11/09, o governo Bush estabeleceu IC como "bens, sistemas e trabalhos vitais para segurança nacional, governança, saúde pública, economia e moral nacional". Os setores de infraestrutura eram: alimentos, água, agricultura, sistemas de saúde e serviços de emergência; energia, transporte, informação e das telecomunicações; bancário e financeiro; de energia, química, indústria da defesa, postal e transporte; e ícones e monumentos nacionais (MOTEFF, 2010).

[1] Estrutura semelhante ao Ministério da Justiça no Brasil.

Ainda na administração Bush, em 2002, quando do lançamento da Estratégia Nacional de Segurança Interna, a definição adotada foi a preparada pelo Congresso americano[2]: "sistemas e recursos, tanto físicos ou virtuais, tão vitais para os Estados Unidos que a incapacidade ou a destruição de tais sistemas e ativos teria um impacto debilitante sobre a segurança econômica nacional, a segurança nacional e a saúde pública, ou qualquer combinação desses elementos". Aqui houve uma distinção entre IC e ativos chaves, os quais foram definidos como estruturas individuais cuja destruição não coloque em risco os sistemas vitais, mas poderia criar desastre local ou danos profundos à moral e confiança da nação, como o monte Rushmore e a Estátua da Liberdade[3]. Esta distinção retirou ícones e monumentos nacionais da lista de setores de ICs americanos (MOTEFF, 2010).

Partindo dessas considerações, este artigo tem como objetivo apresentar a série de ações de proteção das ICs e relacioná-las à atuação do Serviço de Inteligência (SI) de um país. Para além dessa introdução, o texto está dividido em 5 seções, sendo as 4 primeiras o detalhamento das etapas para estabelecer a segurança das ICs. Na última seção, considerações finais são traçadas linhas sobre resultados obtidos, implicações para os governos, limitações do trabalho e sugestões para futuras pesquisas.

2 Etapas de Proteção às ICs

Não há consenso mundial sobre a melhor metodologia para proteger as ICs de um país. Contudo, a partir da análise dos procedimentos realizados por diversos países, como Austrália, Brasil, Canadá, Estados Unidos e União Européia, procurou-se criar um modelo básico das melhores práticas adotadas. Os países foram escolhidos não aleatoriamente, mas por possuírem programas de proteção a IC mais elaborados e por se aproximarem do Brasil na extensão territorial e potencial econômico. A figura 1 abaixo exibe as 4 macro etapas de proteção das ICs.

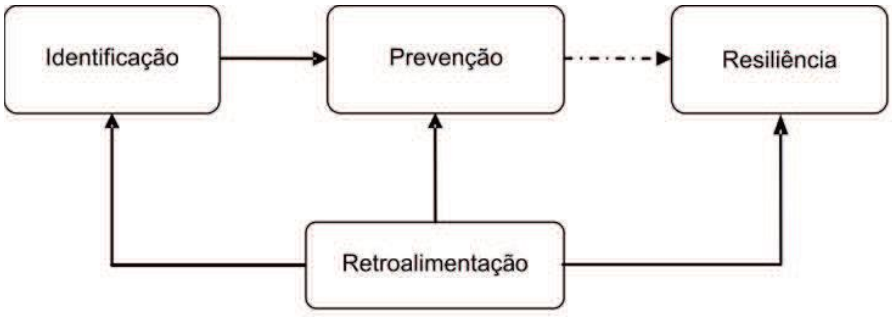

Figura 1: macro etapas de proteção das ICs

[2] *USA Patriot Act* (P.L. 107-56), seção 1016. (ESTADOS UNIDOS, 2001).

[3] No Brasil, caso tivéssemos essa lista de ativos chaves, poderiam estar nela a estátua do Cristo Redentor no Rio de Janeiro e o monumento à Independência do Brasil, em São Paulo, também chamado monumento do Ipiranga.

Primeiramente, são identificadas, dentro do universo de todas as infraestruturas, quais merecem o status de crítica. A seguir elabora-se o plano de prevenção para garantir o contínuo funcionamento da IC. Caso haja um problema, intencional ou não, lança-se mão da etapa de resiliência para que a IC volte a operar normalmente. Como todo processo, há necessidade de contínuo aperfeiçoamento por meio da retroalimentação, uma vez que as ameaças à segurança das ICs também procuram se reinventar.

Muitos são os atores participantes desse processo, o governo em todas as esferas, a iniciativa privada como operadora ou cliente da IC e a população como usuária das ICs, tendo cada um diferentes interesses. Para lidar com essa complexidade, é necessária uma organização central para coordenar a proteção da IC e exigir o comprometimento e ações de todo os envolvidos. No Canadá, esse papel é exercido pelo Ministério de Segurança Pública (PSC), o qual realiza vários programas para garantir a segurança nacional do país, inclusive o Programa para Gerenciamento de Emergências que abarca as ICs canadenses (Public..., 2011). Nos EUA, o Departamento de Segurança Interna (DHS), em conjunto com as Agências específicas de cada setor elencado como área estratégica, são responsáveis por elaborar e implementar o Plano Nacional de Proteção de Infraestruturas (NIPP). Este plano tem o objetivo de proporcionar ao país ICs mais seguras e resilientes (ESTADOS UNIDOS, 2010).

No Brasil, de acordo com a mesma Portaria que definiu o termo IC, o GSI/PR foi designado como coordenador do processo de proteção das ICs. Esta prerrogativa é reforçada no Decreto nº 6.703/2008, que estabelece a Estratégia Nacional de Defesa. (BRASIL, 2008).

3 Etapa de Identificação

Por iniciativa do órgão determinado pelo governo como coordenador do processo, são formados grupos de estudo em cada setor de agrupamento das ICs e definidos os objetivos do processo de proteção das ICs. Por exemplo, nos EUA as ICs ligadas a finanças são de responsabilidade do Departamento de Tesouro, já as ICs de transportes são cobertas pela Administração de Segurança de Transportes do Departamento de Segurança Interna e pela Guarda Costeira para assuntos de transportes marítimos (ESTADOS UNIDOS, 2009). No Brasil foram criados grupos técnicos de acordo com o tema das ICs, por exemplo, para o grupo energia foram criados os seguintes subgrupos: energia elétrica formado por GSI/PR, Ministério das Minas e Energia, Operador Nacional do Sistema Elétrico (ONS) e Agência Nacional de Energia Elétrica (Aneel); Petróleo, Gás Natural e Combustíveis Renováveis formado por GSI/PR, Ministério das Minas e Energia, Agência Nacional de Petróleo (ANP), Petróleo Brasileiro S.A. (Petrobrás), Empresa Brasileira de Pesquisa Agropecuária (Embrapa) (BRASIL, 2010).

As tarefas de definição dos critérios de escolha e seleção de quais estruturas são consideradas críticas são realizadas pelos especialistas de cada área de agrupamento das ICs. Para ilustrar, cita-se o setor de telecomunicações, no qual o Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD) em parceria com a Agência Nacional de Telecomunicações (Anatel) criou uma metodologia para identificar quais são as centrais telefônicas que devem ser protegidas e mantidas em funcionamento no caso de catástrofe natural, como enchentes, ou um evento intencional, como sabotagem. O método adotado é o de pesos e notas, o qual define como critério de escolha níveis de criticidade quantitativo – por exemplo, número de pessoas atendidas - e qualitativo – por exemplo, central que atende serviços essenciais como bombeiros (RIBEIRO et al., 2007).

Este exemplo traz à baila a pergunta sobre quais partes de um ativo necessitam realmente de proteção. De outro modo, num sistema viário, todas as estradas precisam de proteção? Um critério, a princípio mais simples, seria guardar as estradas mais usadas. Porém, esse critério depende de referência, mais usada por quem? Mais usada por veículos em geral ou por veículos de transporte de suprimentos? Outro parâmetro seria o da redundância. Se não houver outra estrada que una dois pontos considerados importantes, tais como local de produção de alimentos e uma cidade populosa, então esse caminho seria considerado crítico. A questão geográfica seria outro critério, por exemplo, considerar apenas estradas que perpassam a capital federal de um país. Por outro lado, também se pode argumentar o uso de um critério setorial, por exemplo, focar apenas nas ICs operadas pela iniciativa privada. Por último cita-se o critério sistêmico, que expõe a complexidade da proteção de ICs. Normalmente há uma dependência ou interdependência entre as ICs. Voltando ao exemplo das centrais telefônicas, elas não funcionam sem a energia elétrica e na eventualidade de manutenção, o processo seria mais rápido se as estradas de acesso a estas centrais também estivessem em bom estado. Destarte, há inúmeros conjuntos de critérios de escolha, sendo mais importante nesse momento determinar o critério técnico mais coerente com os objetivos estabelecidos para proteção das ICs.

Deste contexto depreendem-se alguns alertas na confecção de uma lista de ICs. Há tendência de estender a lista a quase todos os elementos de uma IC, contudo o custo de proteção se torna proibitivo, tornando-se necessária a priorização do mais relevante. Outra questão a lembrar é não deixar o critério político se sobrepor ao critério técnico. Além disso, deve-se atentar para a proteção de ICs que se encontram no exterior. O site Wikileaks (2010) divulgou recentemente documentos sigilosos da diplomacia norte-americana em que consta uma lista de locais vitais aos EUA em outros países, inclusive no Brasil[4]. Para os europeus,

[4] No Brasil, o documento enviado pelo Departamento de Estado americano lista cabos de comunicação submarinos com conexões em Fortaleza e no Rio de Janeiro e minas de minério de ferro, manganês e nióbio em Minas Gerais e em Goiás.

certamente figura em sua lista de ICs o gás proveniente da Rússia e para os brasileiros poderia também constar o gás da Bolívia. O dilema é como proteger uma IC fora de seus domínios. Uma saída seria elaborar listas em conjunto com países em que se tenha mais integração. Assim é feito na União Europeia, em que cada país tem sua lista, mas há também uma lista geral do continente em que todos devem se esmerar para proteger (COMISSÃO..., 2006). Na América do Sul, poderia se pensar em uma lista de ICs do Mercosul ou da União de Nações Sul-Americanas (Unasul), para ser mais abrangente. A lição mais importante é que a partir de critérios bem definidos e rígidos se processe a escolha de quais unidades serão elencadas como IC.

4. Etapa de Prevenção

Nesta etapa a primeira tarefa é entender o que é risco no contexto das ICs. Risco (RIC) é função da probabilidade (P) de uma dada fonte de ameaça explorar um determinado potencial de vulnerabilidade (A->V), acarretando conseqüências danosas (C) a IC e a seus usuários. O risco não pode prescindir de nenhum desses elementos.

$$R_{IC} = f\ (P_{A->V,} C)$$

Ameaça é a ocorrência natural ou provocada por falha, ou, ainda, ocasionada por uma entidade (indivíduo, organização ou nação) doméstica ou estrangeira que possui capacidade e intenção (propósito e motivação) de explorar uma determinada vulnerabilidade da IC. Mais especificamente, a ameaça pode ser natural, não intencional por falha humana ou falha tecnológica ou, ainda, intencional – ver quadro 1 (ESTADOS UNIDOS, 2009; DUNN; WIGERT, 2004; CANADIAN..., 2003).

Tipos de ameaças		Exemplos
Natural		Terremoto, enchentes, deslizamento de terras, furacão, tempestade de raios, etc.
Não intencional	Falha humana	Negligência, imprudência e imperícia
	Falha tecnológica	Erro na programação de um software, mau funcionamento de um equipamento eletrônico, etc.
Intencional		Terrorismo, grupo social reivindicatório, ataque criminoso, guerra declarada, etc.

Quadro 1: Tipos de Ameaças e exemplos

Vulnerabilidade é uma característica física ou atributo operacional que torna uma IC suscetível à exploração de um determinado perigo, ou seja, de ser atacado. Vulnerabilidades podem estar associadas: a fatores físicos, por exemplo, uma cerca quebrada; virtuais, a falta de um firewall; ou humanos, guardas não treinados (ESTADOS UNIDOS, 2009; BRUNNER; SUTER, 2008; DUNN; WIGERT, 2004; CANADIAN..., 2003).

Probabilidade, como o próprio nome sugere, é a chance de que um ataque seja bem sucedido, uma vez tentado por uma ameaça intencional. Para efeitos de cálculo do risco, a probabilidade é estimada em função da ameaça e da vulnerabilidade. Dito de outra forma, avalia-se qual a possibilidade de que uma ameaça, a partir de sua capacidade e intenção, explore uma vulnerabilidade de uma IC. No caso de ameaças naturais e não intencionais, estima-se a probabilidade de acordo com os estudos da área de conhecimento. Por exemplo, para o caso de mau funcionamento de um equipamento eletrônico há o tempo médio de reparo (Mean time to repair - MTTR).

Conseqüência é o efeito de um evento ou incidente; reflete o nível, duração e natureza da perda resultante dessa ocorrência. Grosso modo o impacto quantitativo seria perda de receita, custo de reparo e nível de esforço requerido para isso, já o impacto qualitativo seria a perda de confiança. Para o NIPP (ESTADOS UNIDOS, 2009), as conseqüências são divididas em 4 categorias principais: segurança e saúde pública (epidemias e perdas de vidas), econômica (direta e indireta), psicológica e impactos na governança do país. No Canadá, os fatores considerados são escopo (área geográfica), magnitude (grau do impacto), e efeitos no tempo (DUNN; WIGERT, 2004). Do mesmo modo, na Inglaterra se usa uma escala para quantificar o impacto em 3 fatores: área, severidade e tempo (BRUNNER; SUTER, 2008).

O risco total envolvido na operação de uma IC é avaliado como a soma dos riscos associados a cada um dos possíveis eventos em que as ameaças estejam aptas a explorar as vulnerabilidades e causar consequências destruidoras ($\sum Ri\ i=1$ a n, sendo n o número de cenários possíveis de sinistros da IC). Atentar para o risco cumulativo de efeito cascata das consequências – exemplo, um apagão elétrico em uma cidade tem impacto nas comunicações, que por sua vez impacta no atendimento dos serviços essenciais de saúde e segurança.

A avaliação de risco pode ser representada por um gráfico probabilidade X consequências (ver fig. 2). Cada ponto do gráfico representa uma ameaça que possa explorar determinada vulnerabilidade, e a esse ponto correspondem uma probabilidade de ocorrer (eixo Y) e um grau de severidade da consequên-

cia (eixo X)[5]. Por exemplo, em caso de guerra, um sabotador do país inimigo (ameaça) tem grande chance (probabilidade) de explorar a conivência de funcionários insatisfeitos (vulnerabilidade) e perpetrar um ataque a uma usina nuclear (IC), causando a interrupção de seu funcionamento e consequente geração de energia elétrica, além de vazamentos radioativos (consequências).

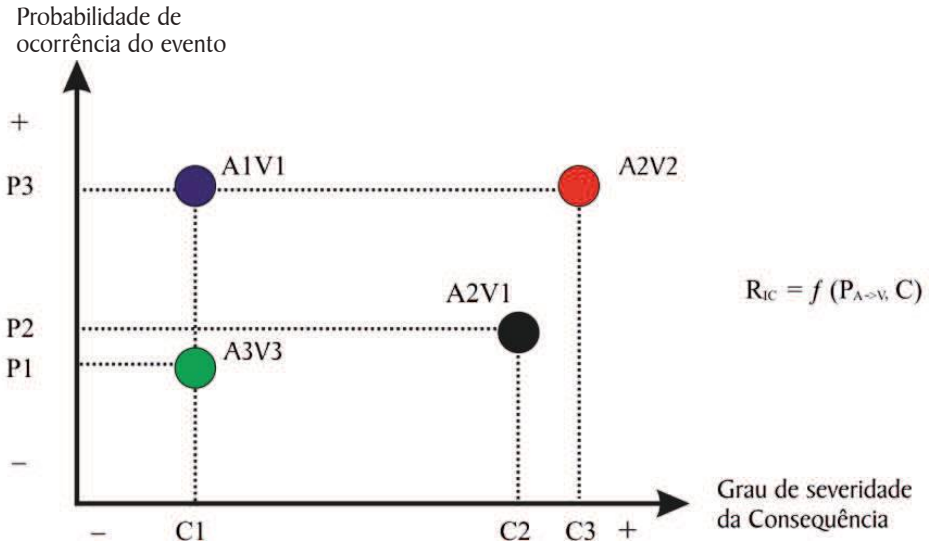

Figura 2: mapeamento de risco de uma IC

A partir da avaliação das medidas de segurança já existentes, o mapeamento do risco cabe ao detentor ou operador da IC e aos órgãos especializados em segurança. Por exemplo, ao Corpo de Bombeiros a prevenção de incêndio, às polícias estaduais, os ataques criminosos. O Serviço de Inteligência pode atuar como mais um órgão de segurança, especializado em antiterrorismo[6], por exemplo, ou até liderando o processo de consolidação das estimativas de risco como acontece na Austrália.

No Brasil, a Agência Brasileira de Inteligência (Abin) vai além e disponibiliza aos órgãos da administração pública e empresas nacionais o Programa Nacional de Proteção do Conhecimento Sensível (PNPC) que é um instrumento preventivo para a proteção e salvaguarda de conhecimentos sensíveis de interesse da sociedade e do Estado brasileiros[7].

Em seguida à avaliação dos riscos procede-se a elaboração do plano de ação

[5] No exemplo hipotético do gráfico da figura 2, o ponto A1V1 (ponto azul) expressa um evento em que a ameaça A1 pode explorar uma vulnerabilidade V1, causando uma consequência C1 com a chance de acontecer P3. A mesma probabilidade P3 se aplica ao evento que pode ser causado pela ameaça A2, explorando a vulnerabilidade V2 (ponto vermelho), porém motivando uma consequência com maior grau de severidade C3. Por outro lado, a mesma ameaça A2, desta vez explorando a vulnerabilidade V1 (ponto preto), causaria um impacto mediano C2 e teria probabilidade de ocorrer P2. Por último, o ponto verde representa o evento em que uma terceira ameaça A3, explorando outra vulnerabilidade V3, provocaria uma consequência C1 e teria a probabilidade menor de ocorrer P1.

[6] Antiterrorismo: conjunto de medidas preventivas voltado para reduzir vulnerabilidades da população, das instituições e da IC, em relação a possíveis atentados terroristas. Contraterrorismo: medidas repressivas executadas para impedir ou mesmo responder a atos terroristas.

[7] Para maiores detalhes ver BALUÉ; NASCIMENTO, 2006.

de defesa para evitar a ocorrência de sinistros. Esse plano é atribuição dos detentores ou operadores da IC. Nesse ponto, mais uma vez, é importante o conceito de priorização para concentrar os esforços nos perigos mais iminentes. Retomando a figura 2, o plano de ação de defesa deve começar pelos eventos do canto superior direito por serem situações de maior probabilidade e consequências mais arrasadoras. No exemplo hipotético, do ponto A2V2, em direção ao canto inferior esquerdo, ponto A3V3. As forças de segurança também apoiam a confecção do plano de segurança, inclusive o SI, principalmente quando se consideram as ameaças intencionais. No Brasil, novamente cita-se o exemplo do PNPC, e também o Programa Nacional de Integração Estado-Empresa na Área de Bens Sensíveis (Pronabens) que tem como função orientar o empresariado brasileiro sobre os controles governamentais para a transferência de tecnologias sensíveis e materiais de uso dual[8].

Concomitantemente aos passos citados acima é necessário o monitoramento do ambiente para antecipar as ações promovidas pelas ameaças, bem como o surgimento de novas ameaças. Nesta fase a atuação do aparato de segurança governamental, em especial o SI[9], é fundamental para prevenir ataques de ameaças intencionais. Relativamente a ameaças naturais, sempre que possível, conta-se com sistemas de monitoramento do clima.

Um óbice à etapa de prevenção se refere à dificuldade de prever o surgimento e desenrolar de distúrbios sociais, incluindo manifestações de grupos sociais que se desviam da conduta reivindicativa e passam a ser consideradas convulsão social (RENN; JOVANOVIC; SCHRÖTER, 2011). Para ilustrar, os distúrbios nos arredores de Paris em 2005, a invasão da Usina Hidrelétrica de Tucuruí na cidade de mesmo nome em 2007 por parte de trabalhadores rurais sem terra e os tumultos em Londres e outras cidades britânicas em 2011. O evento se torna ainda mais complexo quando acontece fora do país detentor ou dependente da IC, como no caso da invasão das instalações da Petrobrás na Bolívia. Para amenizar a incerteza, torna-se necessário um acompanhamento constante e rigoroso do ambiente.

Outro problema a se enfrentar quando da elaboração do plano de prevenção, é a integração com empresas privadas que são operadoras das ICs e que muitas vezes não dispõem de pessoal qualificado ou vontade política para elaborar um planejamento de proteção de suas instalações e serviços. Nesse caso, tornam-se necessárias mudanças na legislação a fim de tornar obrigatória essa prática.

[8] Informações no site da Abin: www.abin.gov.br.

[9] O SI pode atuar de forma passiva monitorando o ambiente e informando à autoridade coordenadora do processo de proteção das ICs e as autoridades responsáveis pela repressão de ilícitos, como as polícias estaduais e federal, e de forma ativa, por exemplo, na busca por terroristas.

Por fim, a comunicação entre os atores do processo, empresas privadas, órgãos de governo, agências reguladoras e forças de segurança, pode se tornar um gargalo na defesa da IC, caso não esteja bem planejada. Nos EUA, para a iniciativa privada há um Centro de Análise e Compartilhamento de Informações (ISAC) para cada setor de ICs e um ISAC central que se comunica com o Centro Nacional de Proteção de Infraestrutura do *Federal Bureau of Investigation* (FBI), o qual atende os órgãos governamentais. Estes centros são responsáveis por receber, analisar e facilitar o compartilhamento de informações entre os atores do processo de proteção das ICs (ESTADOS UNIDOS, 2010).

De forma geral os passos da etapa de prevenção de risco podem ser assim resumidos: diagnóstico da situação atual referente às medidas de prevenção existentes; mapeamento dos riscos; elaboração do plano de ação de defesa; e monitoramento do ambiente.

5 Etapa de Resiliência

Esta etapa possui 3 objetivos: mitigar os efeitos imediatos do sinistro em relação à população atingida; simultaneamente, reagir ao evento causador do desastre, quando for o caso, para que cesse seus efeitos; e reconstruir a IC para que volte a operar normalmente. Para tal, o detentor ou operador deve elaborar planos para cada IC, como na etapa anterior. O órgão coordenador do processo de proteção de ICs se encarrega de incitar os atores a preparar esse planejamento. Para ilustrar, na Europa, cada estado membro deve se assegurar de que para cada IC exista um oficial de ligação de segurança ou equivalente, e um Plano de Segurança do Operador (OSP) que contém as medidas de prevenção e restabelecimento das funcionalidades da IC (COMISSÃO..., 2006).

... os passos da etapa de prevenção de risco [...] diagnóstico da situação atual referente às medidas de prevenção existentes; mapeamento dos riscos; elaboração do plano de ação de defesa; e monitoramento do ambiente.

De modo sucinto, para exemplificar esta etapa, cita-se o atentado a bombas, perpetrado por terroristas, em estações de trens em Madri, na Espanha, em março de 2004, o qual provocou dezenas de mortos e feridos, além de atingir uma IC do setor de transportes[10]. Como forma de mitigar a sensação de medo da população e o sofrimento dos feridos, o governo espanhol empregou um policiamento ostensivo e todos os feridos foram encaminhados a hospitais da região. Para reagir à causa do evento, a polícia mais uma vez foi acionada e, com apoio do SI e demais órgãos de segurança, algumas bombas foram desativadas. Além disso, procedeu-se uma investigação para indi-

[10] O objetivo dos terroristas não foi debilitar a IC, e sim, compelir o governo espanhol a agir conforme determinadas instruções. Mesmo assim, o exemplo ainda é útil, pois como efeito secundário dos atentados houve danos a IC.

car os culpados, ação que culminou em um julgamento em 2007. Paralelamente a isso, o operador do sistema ferroviário dos trens e estações afetados executou as ações para restabelecimento do serviço no mais curto espaço de tempo possível.

No Brasil, caso um sinistro em uma IC venha a acarretar uma crise, existe um Gabinete de Gerenciamento de Crise estabelecido na Secretaria de Acompanhamento e Estudos Institucionais (SAEI) no GSI/PR. Fruto da inoperância governamental em um incêndio de grandes proporções em Roraima em 1998, o gabinete foi criado como um foro de articulação para temas com potencial de crise que envolvam dois ou mais ministérios com o objetivo de prevenir e gerenciar crises. O Gabinete já atuou em diversas ocasiões, como na organização da ajuda humanitária para as vítimas do tsunami de dezembro 2004 na Ásia, na tarefa de minimizar os efeitos de diversas greves de caminhoneiros e na coordenação de atividades para que as grandes manifestações políticas na Esplanada dos Ministérios ocorressem de forma pacífica. Nas ações do Gabinete, o papel da Inteligência tem destaque em antecipar problemas que poderão acontecer e no fornecimento de informações que orientem as decisões das autoridades relacionadas à crise (COUTO; SOARES, 2007).

Como na etapa anterior, o SI continua atuando em monitoramento do ambiente e disponibilização de informações para que sejam atingidos os objetivos da Etapa Resiliência, com destaque para a mitigação dos problemas imediatos e a reação à fonte de ameaça. O sinistro de uma IC pode causar pânico e caos e, nesse momento, ter as informações corretas[11] sobre a situação real faz toda a diferença.

6 Etapa de Retroalimentação do Processo

A etapa de Retroalimentação é recorrente no processo de proteção de ICs de todos os países estudados, uma vez que a constante evolução tecnológica torna necessária uma adaptação nos planos de proteção das ICs. Assim, é preciso sempre revisar o processo, pesquisar novos meios de proteção e educar os envolvidos no processo para a máxima efetividade do sistema de proteção.

A revisão é a medida da efetividade dos planos estabelecidos e abrange todas as etapas do processo, desde a escolha de critérios até o planejamento da recuperação da IC. Isto inclui a Etapa Resiliência, a qual só viria a ser implementada em caso de sinistro na IC. Ou seja, mesmo que a etapa Resiliência nunca tenha sido utilizada, ela deve ser revisada como todas as outras etapas.

A pesquisa está intrinsecamente ligada à revisão. Ela pode tanto servir como gatilho para uma revisão a partir de uma nova descoberta ou invenção, quanto ser o fruto dela após a constatação de uma falha no processo de proteção. Por exemplo, a área de Tecnologia da Informação, que perpassa todos os setores de ICs, está em permanente condição de desenvolvimento. Isto gera necessidade

[11] Valores da informação: disponibilidade, integridade e autenticidade.

de alterações no modo de se proteger uma IC, como estabelecer novas configurações em um antivírus devido a descoberta de novo *malware*[12].

Por meio de palestras, seminários ou cursos, o público envolvido na proteção de ICs deve ser sensibilizado quanto a importância dessa proteção e instado a colaborar com as pesquisas de aperfeiçoamento do processo. A disseminação da informação proporciona um aprendizado mais rápido - um erro em um planejamento pode servir de lição em outras situações.

O SI, como não poderia ser diferente, precisa colaborar com todos os órgãos responsáveis envolvidos. Seja na revisão de seus processos internos para melhor se adequar às mudanças no processo de proteção, seja no auxílio a outras instituições na revisão de seus processos. Também contribui no desenvolvimento de pesquisas, principalmente para aquelas relativas à segurança[13].

7 Considerações Finais

Feitas as apreciações acima, é apresentado a seguir o quadro 2 sobre atuação do SI de acordo com as etapas do processo de proteção das ICs. O SI coopera com os órgãos competentes em quase todas as fases, podendo ficar restrita sua atuação na etapa Identificação e parte da Retroalimentação, que normalmente fica a cargo da entidade coordenadora e especialistas de cada setor, além da fase de recuperação da operação da IC que cabe ao operador.

Salienta-se também que a cooperação do SI não é linear e ocorre em graus diferentes. Por exemplo, sua atuação pode ser mais evidente no monitoramento do ambiente e resposta à fonte de ameaça do que na revisão de processos. Segundo Kent (1967), o SI deve se assemelhar a uma universidade e a um grande jornal, a primeira característica se aplica na etapa Retroalimentação e a segunda, com mais ênfase, na etapa Prevenção.

Etapas		Atuação do SI
Identificação	Definição de critério de escolha	
	Escolha das ICs	
Prevenção	Diagnóstico da situação atual	X
	Mapeamento de riscos	X
	Elaboração do plano de ação de defesa	X
	Monitoramento do ambiente	X
Resiliência	Mitigação dos problemas	X
	Resposta a fonte de ameaça	X
	Recuperação da operação da IC	
Retroalimentação	Revisão de processos	X
	Pesquisa de novos meios de proteção	X
	Educação dos envolvidos	

Quadro 2: atuação do SI na proteção de ICs

[12] *Malware* é um programa de computador cuja finalidade é se infiltrar em computador alheio de forma ilícita para causar algum dano ou roubo de informações.

[13] O Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC), órgão ligado a Abin e ao Ministério da Ciência e Tecnologia (MCT), desenvolve pesquisas para proteger as comunicações mais sensíveis do governo brasileiro. Como exemplo o emprego de criptografia, cuja tecnologia é utilizada no voto eletrônico do Sistema Eleitoral Brasileiro.

A problemática do artigo gera implicações de alerta para que os Estados e respectivos SIs desenvolvam e adaptem iniciativas existentes para proteger as ICs do país. A tendência é o crescimento da importância das ICs devido a sua utilidade e conseqüente necessidade de proteção. Como exemplo, os serviços de informática do governo, conhecidos como e-government, cuja inoperância causaria transtornos como atrasos ou até mesmo a paralisação total de seu funcionamento nas repartições públicas devido ao congestionamento de usuários.

Este estudo levantou questões que não puderam ser estudadas em profundidade nesta fase, pois a finalidade do artigo foi abordar a proteção de ICs e a contribuição dos SIs de forma resumida e elementar para embasar futuras discussões. Em função disso, sugere-se uma aproximação com a academia para investigar temas como: a análise da adequação da classificação das ICs por setor como a melhor forma de agrupamento, tendo em vista a interdependência entre elas; elaboração de leis para amparar a atuação de órgãos governamentais na proteção das ICs, a começar pela lei de greve dos serviços essenciais[14]; e a avaliação da necessidade de cada estado ou município fazer a sua própria lista de ICs.

O estabelecimento de convênio com instituições de pesquisa pode também aprimorar a estratégia de comunicação entre entes envolvidos no sinistro, bem como para a população, a partir dos estudos de transmissão de mensagens em caso de epidemia. Ainda na linha de interesse da atividade de Inteligência, indicam-se estudos comparativos sobre a elaboração de listas de ICs conjuntas com outros países e os impactos na ingerência da soberania alheia.

Referências

AUSTRÁLIA. Trusted information sharing network for critical infrastructure resilience. *Australian Government's Critical Infrastructure Resilience Strategy:* Austrália, 2010. Disponível em: <http://www.tisn.gov.au/Pages/Publications-a-z.aspx>. Acesso em: 20 set. 2011.

BALUÉ, Isabel Gil; NASCIMENTO, Marta Sianes Oliveira do. Proteção do Conhecimento: uma questão de Contra-inteligência de Estado. Revista Brasileira de Inteligência, Brasília, v. 2, n. 3, p. 89-94, set. 2006.

BRASIL. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. *Diário Oficial [da] República Federativa do Brasil.* Brasília, DF. Disponível em: <www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6703.htm>. Acesso em: 10 fev 2012.

BRASIL. Gabinete de Segurança Institucional. *Portaria nº 2, de 8 de fevereiro de 2008.* Brasil, 2008. Institui Grupos Técnicos de Segurança de Infraestrutura Críticas (GTSIC) e dá outras providências. *Diário Oficial [da] República Federativa do Brasil.* Brasília, DF. Disponível em: <http://www.biblioteca.presidencia.gov.br/area-presidencia/pasta.2008-10-08.1857594057/pasta.2009-03-20.4393944761/pasta.2009-03-243858627784/pasta.2009-08-06.2098708078/pasta.2009-08-067125814726/PRT%20n.2%20fev%202008%20GSI.pdf>. Acesso em: 20 mar. 2012.

[14] Lei nº 7.783, de 28 de junho de 1989. (BRASIL, 1989).

BRASIL. Gabinete de Segurança Institucional. *Grupos de infraestruturas críticas,* GSI/PR. Brasil, 2010. Disponível em: <http://www.gsi.gov.br/ infraestruturas-criticas>. Acesso em: 10 ago. 2010.

BRASIL. Lei nº 7.783, de 28 de junho de 1989. Dispõe sobre o exercício do direito de greve, define as atividades essenciais, regula o atendimento das necessidades inadiáveis da comunidade, e dá outras providências. *Diário Oficial [da] República Federativa do Brasil.* Brasília, DF, 29 jun. 1989.

BRUNNER, E. M.; SUTER, M. *International critical information infrastructure protection handbook 2008/2009.* Zurique: Swiss Federal Institute of Technology, 2008.

CANADIAN INTELIGENCE RESOURCE CENTRE. *Office of critical infrastructure protection and emergency preparedness.* Threats to Canada's Critical Infrastructure TA03-001, *2003.* Disponível em: <http://www.publicsafety.gc.ca/prg/em/ccirc/_fl/ta03-001-eng.pdf>. Acesso em: 10 jan. 2012.

COMISSÃO DAS COMUNIDADES EUROPÉIAS. *Comunicação da comissão:* relativa a um Programa Europeu de Protecção das Infra-Estruturas Críticas, 2006. Disponível em: <http://eur-lex.europa.eu/ LexUriServ/ LexUriServ.do?uri=COM: 2006:0786: FIN:PT: PDF>. Acesso em: 21 set. 2011.

COUTO, J. A. C.; SOARES, J. A. M. *Lições de gerenciamento de crises.* Brasília, 2007. Disponível em: <http://www.planalto.gov.br/gsi/saei/publicacoes/licoesGerenciamentoCrises.pdf>. Acesso em: 29 set. 2011.

DUNN, M.; WIGERT, I. *International critical information infrastructure protection handbook 2004.* Zurique: Swiss Federal Institute of Technology, 2004.

ESTADOS UNIDOS. Department of Homeland Security. *National Infrastructure Protection Plan.* Washington, DC, 2009. Disponível em: <www.dhs.gov/nipp>. Acesso em: 21 set. 2011.

ESTADOS UNIDOS. Department of Homeland Security. *Critical infrastructure.* Washington, DC, 2010. Disponível em: <http://www.dhs.gov/files/programs/gc_1189168948944.shtm>. Acesso em: 20 set. 2011.

FRANÇA. *Décret n° 2006-212 du 23 février 2006.* Relatif à la sécurité des activités d'importance vitale. Disponível em: <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000634536&dateTexte=>. Acesso em: 20 set. 2011.

KENT, Sherman. *Informações estratégicas.* Rio de Janeiro: Biblioteca do Exército, 1967.

MOTEFF, John D. *Critical infrastructures:* background, policy, and implementation. Washington, DC: Congressional Research Service, 2010.

PUBLIC SAFETY CANADA. *Critical infrastructure.* 2011. Disponível em: <http://www. publicsafety.gc.ca/prg/em/ci/index-eng.aspx>. Acesso em: 20 set. 2011.

RENN, O.; JOVANOVIC, A.; SCHRÖTER, R. *Social unrest.* Stuttgart: EU-VRi, 2011. (OECD/IFP Project on "Future Global Shocks").

RIBEIRO, Sergio et al. Aplicação da metodologia para identificação da infra-estrutura crítica (MI^2C) no Pan 2007. *Cadernos CPqD Tecnologia,* Campinas, v. 3, n. 2, p. 7-16, 2007.

WIKILEAKS divulga lista de locais 'vitais' para segurança nacional dos EUA. *Uol noticias:* últimas noticias, 06 dez. 2010. Disponível em: <http://noticias.uol.com.br/bbc/2010/12/06/wikileaks-divulga-lista-de-locais-vitais-para-seguranca-nacional-dos-eua.jhtm>. Acesso em: 09 dez. 2010.