Identificação de Infraestrutura Crítica de Telecomunicações com a Metodologia MI^{2}C

Sandra M. Campanholi Tome, Marcos B. Trindade, Sérgio L. Ribeiro, Christiane M. S. Cuculo, Leonardo M. Lage, Eliana de Martino e Regina M. de Felice Souza

***Resumo*— Uma sucessão de eventos naturais ou devidos à ação humana tem levado governos a se preocupar com a proteção de infraestruturas críticas, das quais as telecomunicações fazem parte. Este trabalho apresenta uma metodologia para identificação da infraestrutura crítica de telecomunicações, parte integrante do projeto "Proteção da Infraestrutura Crítica de Telecomunicações" coordenado pela Anatel e desenvolvido pela Fundação CPqD, utilizando recursos do Fundo para o Desenvolvimento Tecnológico das Telecomunicações (FUNTTEL).**

***Palavras-chave*— Infraestrutura crítica de telecomunicações, proteção de infraestrutura crítica, metodologia de proteção de infraestrutura crítica.**

***Abstract*— A series of natural disasters or those due to human action have brought governments worldwide to be concerned about protection of their critical infrastructures, among them the telecommunication infrastructure. This paper presents a methodology for discovering critical points in a telecom infrastructure. That methodology is part of Critical Telecommunications Infrastructure Protection, developed by CPqD under Anatel (Brazilian Telecommunication Regulatory Agency) coordination and sponsored by Telecommunication's Technology Development Fund (FUNTTEL).**

***Keywords*— Critical telecommunications infrastructure, critical infrastructure protection, methodology for critical infrastructure protection.**

I. INTRODUÇÃO

A tensão geopolítica prevalecente no século passado, especialmente em torno da II Guerra Mundial, levou a maior parte dos países a considerar uma série de facilidades tecnológicas como aspectos vitais de sua infraestrutura nacional, visando a segurança política, econômica e sobretudo militar. Data dessa época a proposta pioneira de Paul Baran, no sentido de construir uma rede distribuída (*mesh*), de modo a possibilitar uma recuperação pós-ataque inimigo [1]. Por essa mesma razão, essas tecnologias foram operadas, na maior parte dos casos, por empresas estatais de abrangência nacional, como no caso das telecomunicações, energia e estradas, para citar alguns exemplos. No final do século, face a uma série de mudanças especialmente no ambiente econômico, essas infraestruturas perderam o caráter de segurança nacional, passando a ser vistas como "serviços de utilidade pública" a serem exploradas por empresas privadas, idealmente em regime de concorrência, com o Estado eximindo-se de continuar a participar em sua prestação. Entretanto, o desencadeamento de uma série de ações terroristas, como o "11 de setembro" (de 2001) nos Estados Unidos, tem levado uma série de países a reconsiderarem o aspecto estratégico do funcionamento dessas infraestruturas, visando a preservação da segurança das pessoas e a continuidade das atividades econômicas [2].

No Brasil, a reconsideração da importância das telecomunicações como uma infraestrutura crítica tem origem por volta de 2004, quando a Anatel, em conjunto com o CPqD, iniciou um projeto de pesquisa sobre o tema, na época intitulado Segurança da Rede Nacional de Telecomunicações [3]. Em 2006, o Gabinete de Segurança Institucional da Presidência da República (GSI-PR) amadureceu a noção da importância da segurança da infraestrutura crítica, e estabeleceu naquele período diretrizes para diversas agências do governo e propôs, como um primeiro exercício, a identificação da infraestrutura crítica no município do Rio de Janeiro devido à realização dos Jogos Pan-americanos e Parapan-americanos [4] que aconteceriam no ano seguinte.

Dessa forma, o trabalho de proteção de infraestruturas críticas busca preservar a integridade dessas infraestruturas, senão em sua totalidade, pelo menos em seu "núcleo básico", de modo que a ocorrência de eventos naturais (como terremotos, enchentes ou incêndios em grande escala [5]) ou ações humanas (como ataques terroristas) não interrompam o funcionamento de setores vitais da sociedade atendidos por tais infraestruturas.

Observa-se assim a retomada das questões de segurança em moldes como aqueles preconizados por Baran, após um longo hiato. Mas mesmo em nível mundial, os trabalhos nesse sentido são bastante recentes e ainda incipientes. Embora já existam alguns projetos internacionais [6], um conjunto de fatores leva à conclusão de ser desejável o desenvolvimento de uma metodologia nacional nesse sentido [7]. O primeiro fator é a diversidade entre os países, devido a aspectos geográficos, culturais e ao próprio histórico de escolha de tecnologias e implantação das infraestruturas, fazendo com que a metodologia criada para uma dada realidade possa não ser adequada a outra realidade. O segundo fator é a diversidade regional e local, fazendo com que o Brasil apresente uma série

Sandra M. C. Tome, Marcos B. Trindade e Leonardo M. Lage – Diretoria de Redes de Telecomunicações, Fundação CPqD, Campinas, SP, E-mails: {sandrat, trindade, lmlage}@cpqd.com.br.

Sérgio L. Ribeiro, Christiane M. S. Cuculo e Eliana De Martino – Diretoria de Tecnologia de Serviços, Fundação CPqD, Campinas, SP, E-mails: {sribeiro, ccuculo, martino}@cpqd.com.br.

Regina M. F. Souza, ANATEL, Brasília, DF, E-mail: reginas@anatel.gov.br.

de “realidades locais” distintas, requerendo uma metodologia capaz de lidar com essa diversidade, não atendida pelas demais propostas.

Este artigo apresenta os trabalhos em desenvolvimento no CPqD, com coordenação da Agência Nacional de Telecomunicações (Anatel) e patrocínio do Fundo para o Desenvolvimento Tecnológico das Telecomunicações (FUNTTEL), visando criar um conjunto de metodologias para a proteção de infraestruturas críticas. Mais especificamente, dentro desse trabalho, apresenta-se aqui a metodologia para a identificação de tais infraestruturas.

II. Projeto de Proteção da Infraestrutura Crítica de Telecomunicações

A larga disseminação de redes e serviços de telecomunicações, de topologia complexa, resulta em uma sensação de segurança, a qual pode ser ilusória, ocultando perigosas lacunas e fragilidades não negligenciáveis. Esse tem sido o norteador da política que vem sendo estabelecida pelo GSI-PR por meio de sucessivos decretos presidenciais [7], [8], [9]. Conforme a definição formalmente adotada pelo Brasil, uma infraestrutura crítica refere-se a *instalações, serviços ou bens que, se interrompidos ou destruídos, provocarão sério impacto social, econômico, e/ou político, internacional ou à segurança nacional* [7]. Isso inclui, além das telecomunicações, setores como os de energia, transportes, água e finanças, entre outros. Esses setores possuem, em comum, além do fato de servirem de suporte (infraestrutura) a demais atividades econômicas e sociais, o fato de estarem organizados em complexas redes formando interdependências geralmente não óbvias, de modo que uma interrupção ou sobrecarga em determinado segmento pode se propagar rapidamente para os demais, provocando um efeito cascata que pode levar o sistema inteiro ao colapso.

Com a gradual consolidação dos conceitos e melhor compreensão do problema, o escopo vem sendo estendido e foi assim que, a partir de 2007, a Anatel e o CPqD iniciaram um novo projeto, denominado “Proteção da Infraestrutura Crítica em Telecomunicações” (PICT), com o objetivo de:

i) Criar um cenário ideal de proteção da infraestrutura crítica de telecomunicações;
ii) Diagnosticar e analisar os pontos críticos do setor de telecomunicações;
iii) Elaborar propostas para a prevenção de incidentes de segurança e garantir a continuidade das operações após desastres ou falhas de qualquer natureza;
iv) Fornecer subsídios ao País para a formulação de normas, regulamentos, estratégias e políticas para a proteção da infraestrutura crítica de telecomunicações.

Para atingir os objetivos propostos, o Projeto PICT foi subdividido em cinco etapas, cada qual englobando uma metodologia específica, conforme delineado na Fig. 1. A primeira etapa consiste na Metodologia para a Identificação de Infraestrutura Crítica (MI^{2}C). Para sistemas complexos como as atuais redes de telecomunicações, multiplataforma e multisserviços integrados, a identificação dos aspectos ou segmentos críticos dessa infraestrutura não é tarefa óbvia, requerendo uma metodologia que possibilite extrair as informações adequadas e ao mesmo tempo lidar com a diversidade de situações da realidade brasileira.

A segunda etapa consiste na Metodologia para a Identificação e Análise de Ameaças (MIdA^2), a qual aborda a determinação das ameaças que podem causar danos à infraestrutura crítica e a respectiva análise de riscos.

A terceira etapa, Metodologia para Análise de Interdependência entre Infraestruturas Críticas, visa identificar e avaliar a interdependência entre as redes, com o objetivo de, entre outros, evitar a propagação de eventos por efeito cascata e também analisar a interdependência entre a rede de telecomunicações e as demais infraestruturas críticas.

Fig. 1. Metodologias que compõem o Projeto de Proteção de Infraestruturas Críticas (PICT).

A quarta etapa, Metodologia para Criação do Cenário Ideal para Infraestrutura Crítica (M(CI)^{2}C), visa propor um cenário para a efetiva proteção das infraestruturas críticas, o qual implementa todos os controles que possibilitem o funcionamento adequado dos serviços, minimizando a interferência de falhas durante o projeto, implementação e operação, sejam eles devido a fatores naturais ou humanos (maliciosos ou não). A etapa seguinte, Metodologia para Diagnóstico de Infraestrutura Crítica (MeDI^{2}C), visa gerar recomendações para proteção de infraestrutura crítica de telecomunicações e definir um plano de ação baseado na criticidade e prioridade dos riscos mapeados.

Descreve-se a seguir, em maiores detalhes, a primeira metodologia.

III. Metodologia para a Identificação de Infraestrutura Crítica (MI^{2}C)

A identificação e o mapeamento da infraestrutura crítica de telecomunicações correspondem aos primeiros passos para sua proteção efetiva. Para atingir esse objetivo, a Metodologia para a Identificação de Infraestrutura Crítica (MI^{2}C) consiste essencialmente em identificar os elementos de uma infraestrutura de telecomunicações e estabelecer uma classificação dos mesmos a partir da determinação do nível de criticidade dos serviços de telecomunicações, o que é feito com base em aspectos sociais, econômicos e políticos.

Assim, a metodologia MI^{2}C compreende um conjunto de atividades executadas em oito fases, relacionadas a seguir, cujo fluxo de informações é apresentado na Fig. 2.

Fase 1 – Identificação e definição dos serviços de telecomunicações;

Fase 2 – Definição dos aspectos a serem avaliados para cada serviço definido na Fase 1;

Fase 3 – Definição dos níveis de criticidade a serem estabelecidos;

Fase 4 – Definição de pesos para cada aspecto definido na Fase 2;

Fase 5 – Análise dos níveis de criticidade;

Fase 6 – Mapeamento e classificação dos serviços críticos de telecomunicações;

Fase 7 – Identificação e definição da infraestrutura de redes de telecomunicações;

Fase 8 – Mapeamento e classificação dos elementos da infraestrutura crítica de telecomunicações.

Na Fase 1, são identificados todos os serviços de telecomunicações oferecidos pelas prestadoras (e regulados pela Anatel). Na Fase 2, são definidos os aspectos que serão considerados para a avaliação de criticidade de cada serviço de telecomunicações identificado na Fase 1. Esses aspectos podem ser sociais, econômicos ou políticos. Como exemplo de aspecto social tem-se o atendimento de hospitais. Aspectos econômicos referem-se ao suporte às atividades econômicas, tendo como exemplo o atendimento a regiões com grande concentração de empresas. Aspectos políticos referem-se, por exemplo, ao atendimento a regiões de fronteira ou da floresta amazônica.

A Fase 3 tem como objetivo definir níveis de criticidade qualitativos a serem estabelecidos para cada serviço de telecomunicações, para cada aspecto identificado na Fase 2. Os níveis de criticidade irão identificar o índice de influência que cada serviço de telecomunicações exerce sobre determinado aspecto.

A Fase 4 consiste em se estabelecer um peso relativo a ser aplicado em cada fator identificado na Fase 2. Os pesos devem ser definidos de acordo com os interesses específicos da Nação, podendo considerar tanto fatores estruturais ou de longo prazo, como as necessidades de desenvolvimento regional, quanto fatores conjunturais ou de curto prazo, como aqueles ditados pela situação econômica.

Deve-se observar que as Fases 2, 3 e 4 compreendem um certo grau de subjetividade, ou seja, as definições adotadas podem refletir a visão específica de pessoas ou instituições consultadas. Portanto, para evitar distorções, a metodologia é aplicada entrevistando-se os principais atores envolvidos, incluindo os setores governamentais e empresas prestadoras do serviço. Assim, ainda que um fator de subjetividade possa estar presente durante a coleta de dados, ele é diluído e posteriormente eliminado adotando-se os valores médios.

Definidos os serviços, os aspectos e respectivos fatores de ponderação, a Fase 5 consiste em computar e analisar os níveis de criticidade de cada serviço, enquanto na Fase 6 é realizada uma classificação dos mesmos, de modo a identificar um subconjunto de serviços que efetivamente representem aspectos críticos da infraestrutura. A aplicação da metodologia MI^{2}C levou à identificação de três serviços, dentre a totalidade daqueles regulados pela Anatel, pelos critérios de relevância: o Serviço Telefônico Fixo Comutado (STFC), o Serviço Móvel Pessoal (SMP) e o Serviço de Comunicação Multimídia (SCM).

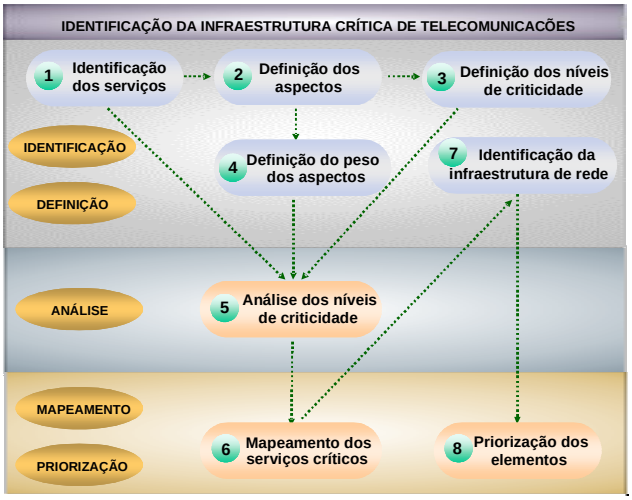

Fig. 2. Metodologia de Identificação de Infraestrutura Crítica (MI^{2}C).

A Fase 7 consiste na identificação das infraestruturas de rede que dão suporte aos serviços críticos de telecomunicações e definição dos critérios para a classificação dos elementos críticos identificados. Nas Tabelas I e II apresentam-se os principais critérios adotados. Foi definido que a granularidade a ser utilizada para comparação de importância na continuidade dos serviços críticos entre as infraestruturas de rede seria a estação de telecomunicações, a qual agrega diferentes elementos de rede.

TABELA I
CRITÉRIOS GEOGRÁFICOS/SOCIAIS/ESTRATÉGICOS

Atendimento (em capitais e cidades >200k hab.)
Setor de saúde
Segurança pública
Órgãos governamentais
Centros financeiros
Transporte (portos e aeroportos)
Setores de energia (subestações, refinarias)
Indústrias

TABELA II
CRITÉRIOS TECNOLÓGICOS

Característica da estação
Ponto de interconexão
Volume de tráfego
Capacidade de transmissão
Quantidade de terminais equivalentes
Funções de sinalização/NGN/Data Center
Gerência de rede
Energia CA/CC/GMG
Compartilhamento da infraestrutura

A Fase 8 tem por finalidade classificar os elementos das infraestruturas de redes de diferentes prestadoras dos serviços críticos de telecomunicações. Uma forma direta de se obter uma classificação seria pela aplicação das notas de cada estação em cada quesito, ponderando-se pelo respectivo peso. Entretanto, esse método trataria de forma igual as realidades de diversas situações. Para contornar tal problema, os critérios são agrupados em categorias, e a comparação é efetuada entre

categorias, não necessariamente entre critérios individuais. Para o cômputo final, a cada categoria é atribuído um peso e um fator de normalização, de modo a manter coerência estatística.

A nota final de cada estação é calculada aplicando-se a equação (1) [4], [10].

$$PS_n = \sum_{i=1}^{K} \sum_{j=1}^{C_i} \alpha_i N_{ij} \quad (1)$$

onde

PS_n = Pontuação final da *n*-ésima estação ou *n*-ésimo site avaliado;

K = Número de categorias;

C_i = Número de critérios da *i*–ésima categoria;

α_i = Fator de normalização da nota em função do peso da *i*-ésima categoria;

N_{ij} = Nota atribuída ao *j*-ésimo critério da *i*-ésima categoria.

O fator de normalização, por sua vez, expressa a razão entre o peso de cada categoria e o somatório das notas máximas dos critérios pertencentes a essa categoria, conforme a equação (2) [4], [10].

$$\alpha_i = \frac{P_i}{\sum_{j=1}^{C_i} N\max_{ij}} \quad (2)$$

onde

α_i = Fator de normalização da nota em função do peso da *i*-ésima categoria;

P_i = Peso da *i*-ésima categoria;

C_i = Número de critérios da *i*-ésima categoria;

$N\max_{ij}$ = Nota máxima atribuída ao *j*-ésimo critério da *i*-ésima categoria.

IV. Aplicação da Metodologia

A metodologia MI^{2}C foi aplicada para a identificação de estações críticas dentre diversas prestadoras dos serviços de telecomunicações no Brasil, que validaram os resultados obtidos, conforme mostra a Fig. 3, apontando em ordem decrescente parte das estações com maior grau de criticidade no Brasil.

Os dados que servem de exemplo à Fig. 3 consideram somente a dimensão tecnológica. Os critérios foram agrupados em cinco categorias nas quais as estações receberam suas pontuações, quais sejam: serviço STFC; serviço SMP; serviço SCM; suporte a transmissão; e demais aspectos de infraestrutura.

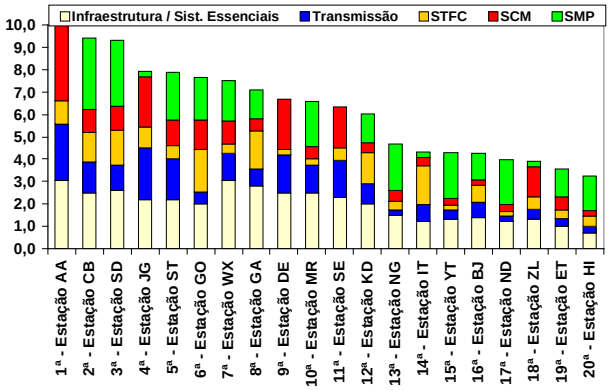

Fig. 3. Pontuação das estações com a aplicação da MI^{2}C[1].

Observa-se, pela Fig. 3, que é possível comparar estações que possuem naturezas díspares, mostrando a flexibilidade e a capacidade da metodologia em lidar com informações provenientes de fontes diversas. A estação mais pontuada, Estação AA, participa da prestação de apenas dois dos serviços de telecomunicações considerados, além de suportar a transmissão de longa distância. Já as quatro estações seguintes (CB, SD, JG, e ST) participam da prestação de todos os serviços considerados. Isto mostra a flexibilidade da metodologia para fazer uma análise mais aprofundada da contribuição da pontuação de cada categoria na nota final da estação. Pode ser verificado que a Estação GO, ordenada em sexta posição pelo critério composto, alcançaria a pontuação máxima caso o enfoque da análise fosse somente o serviço STFC, conforme indicado na Fig. 4.

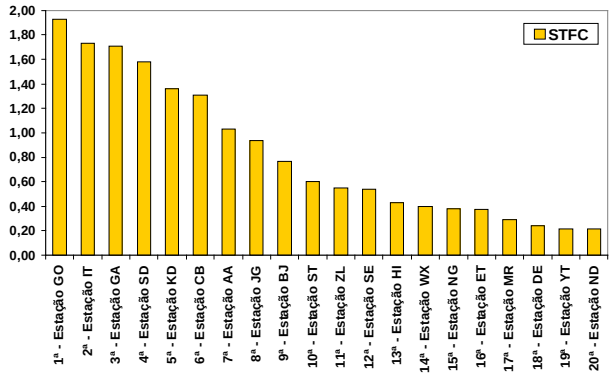

Fig. 4. Pontuação das estações considerando o serviço STFC.

Na Fig. 5 apresenta-se outro exemplo de aplicação da metodologia MI^{2}C – o de identificação das estações críticas para situações de crise, como foi o caso das áreas atingidas pelas enchentes ocorridas no Vale do Itajaí-SC, em novembro de 2008. Filtrando-se os dados relativos às estações que atendem o Vale do Itajaí, obtém-se as estações críticas das três cidades mais atingidas pela catástrofe – Blumenau, Itajaí e Ilhota. Das dez mais críticas, oito estão localizadas em Blumenau, seis das quais encontram-se, conforme indicados por pontos na Fig. 5, nas proximidades do rio Itajaí, o que faz

[1] Como são dados sensíveis, os nomes reais das estações foram substituídos por mnemônicos gerados aleatoriamente.

com que parte de sua criticidade advenha da exposição às enchentes.

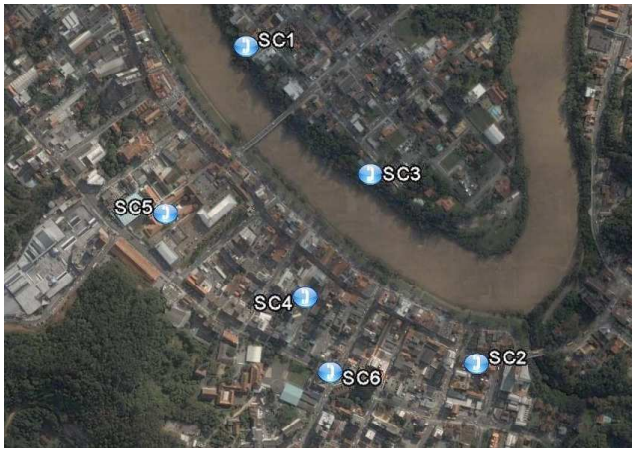

Fig. 5. Estações de telecomunicações de Blumenau[2]

A Fig. 6 mostra as escolas, hospitais, postos de saúde e unidades de utilidade pública, tais como bombeiros, atendidos por essas estações. Assim, verifica-se por esse mapa que, diversas dessas instituições, embora estejam mais afastadas do rio, terão suas comunicações afetadas em caso de enchentes, pelo fato daquelas estações possuírem tal vulnerabilidade.

Fig. 6. Escolas, hospitais e unidades de utilidade pública atendidas pelas estações críticas em Blumenau.

A metodologia MI^{2}C serve, portanto, para identificar quais são as estações mais críticas. A partir de seus resultados, em conjunto com as demais metodologias citadas na seção II, é possível, por exemplo, elaborar um planejamento adequado de prevenção de interrupções ou deterioração dos serviços de telecomunicações mesmo em casos de situação de calamidade pública.

[2] Como são dados sensíveis, por questões de segurança, os pontos marcados não correspondem à localização real das estações. O propósito da ilustração é, portanto, didático.

Outro exemplo de aplicação refere-se à elaboração de um plano adequado de garantia às comunicações na Copa do Mundo de Futebol de 2014, que ocorrerá no Brasil. Em eventos dessa natureza, existe um enorme afluxo de público e uma cobertura intensiva da mídia, gerando um volume de tráfego que irá crescer repentinamente para o período de realização dos jogos. Assim, faz-se necessária a identificação dos possíveis pontos de gargalo nas infraestruturas, telecomunicações inclusive, para minimizar os riscos que possam prejudicar o evento.

V. Conclusões

No curso dos trabalhos, a metodologia foi validada e refinada por meio de sua aplicação junto às prestadoras dos serviços de telecomunicações participantes do projeto. Os resultados alcançados pelo projeto influenciaram na definição formal, realizada pelo Governo Federal em fevereiro de 2008, do significado da expressão "infraestrutura crítica" e na designação do conjunto de infraestruturas consideradas críticas no Brasil (telecomunicações, energia, água, transportes e finanças). Nessa mesma oportunidade, foram instituídos os Grupos Técnicos de Segurança de Infraestruturas Críticas (GTSICs) de Energia e de Telecomunicações.

Pelo fato de, em sociedades modernas, as infraestruturas apresentarem-se como uma complexa rede de nós interligados, os pontos de vulnerabilidade são ocultos pela sua aparente complexidade e, ao mesmo tempo, as interconexões que servem de rotas alternativas podem também servir para propagar os eventos negativos, criando um efeito cascata e levando todo o sistema rapidamente ao colapso. Assim, a proteção adequada de infraestruturas críticas requer, como passo inicial, a correta identificação dos elementos que compõem os seus principais pontos de fragilidade, tarefa não elementar devido à robustez aparente.

A MI^{2}C consegue abstrair a complexa realidade formada por um imenso volume de nós (estações) interligados com múltiplas interdependências e refletindo uma disparidade de realidades regionais, econômicas e políticas, de modo a obter um conjunto reduzido de informações que refletem adequadamente os seus pontos de vulnerabilidade.

Cabe ressaltar que esta metodologia, por ter o papel de abstrair informações com foco em aspectos de segurança e interdependências, pode ser aplicada a outras infraestruturas, tais como as de energia, transporte, etc.

Agradecimentos

O presente trabalho foi desenvolvido em conjunto com a Anatel e suporte financeiro do Funttel – Fundo para o Desenvolvimento Tecnológico das Telecomunicações.

Referências

[1] P. Baran, "Introduction to Distributed Communications Networks", *Rand Memorandum 3420-PR.*, disponível em http://www.rand.org/pubs/research_memoranda/RM3420/RM3420.chapter1.html.

[2] D. Assaf, "Models of critical information infrastructure protection", *International Journal of Critical Infrastructure Protection*, vol. I, 2008.

[3] S. L Ribeiro, E. T. Nakamura and E. K. Bezerra,, "Critical Infrastructure in Brazil", in *1st IEEE International Workshop on Critical Infrastructure Protection*, 2005.

[4] S. L Ribeiro, J. H. A. Franco, M. B. Trindade, E. L. Dias and R. M. F. Souza, "Aplicação da Metodologia de Identificação da Infraestrutura Crítica no Pan 2007", *Caderno CPqD de Tecnologia*, vol. 3, no. 2, 2007.

[5] L. L. Parks, B. D. Kushler, M. J. Serapiglia, L. A. McKenna Jr., E. K. Budnick and J. M. Watts Jr., "Fire Risk Assessment for Telecommunications Central Offices", *Journal Fire Technology*, vol. 34, no. 2, 1998.

[6] T. G. Lewis, *Critical infrastructure protection in homeland security: defending a networked nation*, John Wiley & Sons, 2006.

[7] BRASIL, *Diário Oficial da União (DOU)*, Ano CXLV, no. 27, de 11 de fevereiro de 2008.

[8] BRASIL, *Diário Oficial da União (DOU)*, Ano CXLV, no. 30, de 14 de fevereiro de 2008.

[9] BRASIL, *Diário Oficial da União (DOU)*, Ano CXLV, no. 157, de 15 de agosto de 2008.

[10] M. B. Trindade, S. M. C. Tome, S. L Ribeiro, C. M. S. Cuculo, L. M. Lage, E. Martino e R. M. F. Souza, "Metodologia para Identificação da Infraestrutura Crítica de Telecomunicações e sua Aplicação em Estudo de Caso", *Conferencia Ibero-Americana de Ingeniería e Innovación Tecnológica: CIIIT 200.*, vol. III, 2009.